Rational Reduction of a Pair of Binary Quadratic Forms; their Modular Invariants.

By Leonard Eugene Dickson.

1. The primary object of the present paper is a study of the invariants of a pair of binary quadratic forms under modular transformation. Incidentally, the invariants of a single form are given a more satisfactory expression than hitherto employed (§ 7).

It is shown that the knowledge of a complete set of canonical types of pairs of forms is of great service in the discovery and proof of relations between certain of the modular invariants and in establishing the independence of other invariants (§§ 23, 25).. For these reasons and for the purpose of giving interpretations to the modular invariants, we begin the investigation with a discussion of the necessary and sufficient conditions for the equivalence of two pairs of quadratic forms.

Within the field C of all complex numbers, Weierstrass's elementary divisors enable one to state necessary and sufficient conditions for the equivalence of two pairs of quadratic forms; but for a smaller field contained in C, or for any finite field, these conditions are not sufficient, since the formulae of transformation involves irrationalities. Before stating the additional necessary conditions, we express the above conditions in the following equivalent form. Let θ denote the quadratic simultaneous invariant and j the Jacobian of q_1, q_2; Θ and J those for Q_1, Q_2. If $j \not\equiv 0$, then must

$$| Q_1 | : | q_1 | = | Q_2 | : | q_2 | = \Theta : \theta.$$

But if $j \equiv 0$, so that $q_2 \equiv m q_1$, then must $J \equiv 0$, so that $Q_2 \equiv M Q_1$; and furthermore, m and M must be equal. For a field other than C, the above equal ratios, as well as certain other specified functions of the coefficients, must be squares in the field; further, the leading coefficient of Q_1 must be representable by the form q_1. The latter condition, requiring the solvability of a

diophantine equation, is considerably weaker than the requirement that an indicated square root shall be rational.

For finite fields, the criteria become simpler and are expressed entirely in terms of the invariants of the two forms. When the modulus p exceeds 2, the criteria are that the algebraic invariants $|q_1|$, $|q_2|$, θ of one pair of forms shall equal the products of those of the other pair by the same square, and that four modular absolute invariants have the same values for the two pairs (§ 13). For $p=2$, we again employ three relative invariants, the resultant and the coefficients of xy (which take the place of the determinants), and three absolute invariants (§§ 22, 32).

REDUCTION IN A FIELD F NOT HAVING MODULUS 2, §§ 2–13.

2. Consider two quadratic forms with coefficients in F,

$$q_1 = a_0 x^2 + 2a_1 xy + a_2 y^2, \quad q_2 = b_0 x^2 + 2b_1 xy + b_2 y^2, \tag{1}$$

having the determinants and simultaneous invariant

$$a = a_0 a_2 - a_1^2, \quad b = b_0 b_2 - b_1^2, \quad \theta = a_0 b_2 - 2a_1 b_1 + a_2 b_0. \tag{2}$$

Consider a second pair of forms Q_1, Q_2, with coefficients $A_0, \ldots, B_2$ in F and invariants A, B, Θ. If there exists in F a linear tranformation of determinant Δ which replaces q_1 by Q_1, and q_2 by Q_2, the product of the determinant

$$|\lambda q_1 + \mu q_2| = a\lambda^2 + \theta\lambda\mu + b\mu^2 \tag{3}$$

by Δ^2 equals the determinant

$$|\lambda Q_1 + \mu Q_2| = A\lambda^2 + \Theta\lambda\mu + B\mu^2. \tag{4}$$

Hence a necessary condition for the equivalence of the two pairs is*

$$A : a = \Theta : \theta = B : b = \text{square in } \mathsf{F}. \tag{5}$$

3. First, let q_1 and Q_1 be irreducible in F, viz., let $-a$ and $-A$ be not-squares. In particular, $a_0 \neq 0$, $A_0 \neq 0$. For $x = X - a_1 Y$, $y = a_0 Y$,

$$q_1 = a_0 (X^2 + aY^2), \quad q_2 = b_0 X^2 + 2cXY + dY^2, \tag{6}$$

$$c = a_0 b_1 - a_1 b_0, \quad d = b_0 a_1^2 - 2b_1 a_0 a_1 + b_2 a_0^2. \tag{7}$$

By (5), $a = t^2 A$, t an element in F. For $x = \xi - A_1 t\eta$, $y = A_0 t\eta$,

$$Q_1 = A_0 (\xi^2 + a\eta^2), \quad Q_2 = B_0 \xi^2 + 2C\xi\eta + D\eta^2, \tag{8}$$

$$C = t(A_0 B_1 - A_1 B_0), \quad D = t^2 (B_0 A_1^2 - 2B_1 A_0 A_1 + B_2 A_0^2). \tag{9}$$

---

* In the sense $A = \Delta^2 a$, etc., so that $a = 0$ implies $A = 0$, etc.

Then $X = \alpha\xi + \beta\eta$, $Y = \gamma\xi + \delta\eta$ replaces q_1 by Q_1, if, and only if,

$$a_0(\alpha^2 + a\gamma^2) = A_0, \quad \alpha\beta + a\gamma\delta = 0, \quad a_0(\beta^2 + a\delta^2) = A_0 a.$$

Eliminating β from the last two and applying the first, we get $\delta^2 = \alpha^2$. In every case, we have $\delta = \pm\alpha$, $\beta = \mp a\gamma$. The only further condition is

$$a_0(\alpha^2 + a\gamma^2) = A_0, \tag{10}$$

which states that the form q_1 must be capable of representing A_0. We assume that this necessary condition is satisfied and let α, γ be a particular set of solutions in F of (10). Then

$$X = \alpha\xi - a\gamma\eta, \quad Y = \gamma\xi + \alpha\eta$$

transforms the pair of forms (6) into

$$q_1 = A_0(\xi^2 + a\eta^2), \quad q_2 = e\xi^2 + 2f\xi\eta + g\eta^2, \tag{11}$$

$$\left.\begin{array}{c} e = b_0\alpha^2 + 2c\alpha\gamma + d\gamma^2, \quad f = c\alpha^2 + (d - b_0 a)\alpha\gamma - ca\gamma^2, \\ g = d\alpha^2 - 2ca\alpha\gamma + b_0 a^2\gamma^2. \end{array}\right\} \tag{12}$$

Now $q_1 = Q_1$. Hence any transformation T replacing q_1, q_2 by Q_1, Q_2 must be an automorph of q_1. By the above discussion, T must be of the type

$$\xi = r\xi' \mp as\eta', \quad \eta = s\xi' \pm r\eta', \quad r^2 + as^2 = 1. \tag{13}$$

We proceed to express (13) in parametric form. For $s \neq 0$, we may set

$$r - 1 = \rho s\ (\rho \neq 0), \quad r + 1 = -as/\rho.$$

The resulting values of r, s are given by (14) for $\sigma = 1$:

$$r = \frac{-\rho^2 + a\sigma^2}{\rho^2 + a\sigma^2}, \quad s = \frac{-2\rho\sigma}{\rho^2 + a\sigma^2}. \tag{14}$$

The sets $s = 0$, $r = \pm 1$, are given by (14) for $\sigma = 0$, or $\rho = 0$. Hence the solutions of $r^2 + as^2 = 1$ are given uniquely by (14) with ρ and σ not both zero, so that the denominators do not vanish. Now (13) replaces (11_2) by

$$q_2 = E\xi'^2 + 2F\xi'\eta' + G\eta'^2, \quad E = er^2 + 2frs + gs^2, \tag{15}$$

the values of F and G not being required. In fact, since (13) has determinant ± 1, we have the absolute invariants

$$\Delta \equiv f^2 - eg = F^2 - EG, \quad I \equiv g + ea = G + Ea. \tag{16}$$

As a temporary abbreviation, set

$$k = g - ea, \quad l = \tfrac{1}{4}(E - e). \tag{17}$$

Then by (14) and (15),

$$l = \{ k\rho^2\sigma^2 + f\rho\sigma(\rho^2 - a\sigma^2) \} / (\rho^2 + a\sigma^2)^2. \tag{18}$$

Postponing the cases $\rho = 0$ and $\sigma = 0$, we may take $\rho = 1$, $\sigma \neq 0$. Then (18) is unaltered when σ is replaced by $-1/a\sigma$. Thus we set

$$\varepsilon = \sigma - 1/a\sigma. \tag{19}$$

Then (18) becomes the quadratic equation

$$l(a\varepsilon^2 + 4) = k/a - f\varepsilon. \tag{20}$$

But by (16) and (17),

$$F^2 - f^2 = E(I - Ea) - e(I - ea) = 4l[I - a(E + e)] = 4l(k - 4al). \tag{21}$$

Hence (20) gives

$$(al\varepsilon + \tfrac{1}{2}f)^2 = lk - 4al^2 + \tfrac{1}{4}f^2 = \tfrac{1}{4}F^2,$$

$$\varepsilon = \varepsilon_{\pm} = (f \pm F)/(-2al). \tag{22}$$

By (19) and (20),

$$(\sigma - \tfrac{1}{2}\varepsilon)^2 = (a\varepsilon^2 + 4)/4a = (k/a - f\varepsilon)/(4al). \tag{23}$$

Inserting the value (22) and eliminating k by (21), we get

$$(\sigma - \tfrac{1}{2}\varepsilon)^2 = S_{\pm}/(16a^2l^2), \quad S_{\pm} \equiv (F \pm f)^2 + a(E - e)^2. \tag{24}$$

Hence one of the $S_{\pm}$ must be zero or a square in the field F. The same result holds if $\rho = 0$ or if $\sigma = 0$, since then $l = 0$, $E = e$, $G = g$, $F^2 = f^2$.

THEOREM. *The necessary and sufficient conditions that a pair of quadratic forms* (1), *of which the first is irreducible in the field* F, *shall be equivalent in* F *to a pair* Q_1 *and* Q_2 *are that relations* (5) *shall hold between their invariants, that* A_0 *shall be representable by the form* q_1, *and that one of the expressions*

$$(C \pm f)^2 + a(B_0 - e)^2 \tag{24'}$$

shall be a square in F, *where* C, f, e *are given by* (7), (9), (10), (12).

For a finite field, equation (10) is solvable,* so that A_0 is representable by q_1. Further, the condition on (24′) is satisfied if $-R$ is zero or a not-square, where

$$R = 4ab - \theta^2 \tag{25}$$

is the resultant of (1). Indeed, by (22), (21),

$$\left(\frac{k}{a} - f\varepsilon_+\right)\left(\frac{k}{a} - f\varepsilon_-\right) = \frac{k^2}{a^2} + \frac{kf^2}{a^2 l} + \frac{f^2(f^2 - F^2)}{4a^2l^2} = \frac{k^2 + 4af^2}{a^2}.$$

---

* *Linear Groups*, p. 46.

But by (16), (17), and $I = A_0 \theta$, $\Delta = -A_0^2 b$,

$$k^2 + 4af^2 = (I - 2ae)^2 + 4a(\Delta + Ie - ae^2) = I^2 + 4a\Delta = -A_0^2 R.$$

Hence by (23), (24),

$$S_+ S_- = -16 l^2 A_0^2 R. \tag{26}$$

In a finite field the product of two not-squares is a square; hence if $-R$ is zero* or a not-square one of the $S_\pm$ is zero or a square.

COROLLARY. *In a finite field a pair of quadratic forms* (1), *whose resultant R is zero or the negative of a not-square, and the first of which is irreducible, is equivalent to a second pair if and only if relations* (5) *hold between their invariants.*

4. The case in which $-R$ is a square $\neq 0$ in F, while q_1 is irreducible, may be treated advantageously by a well known method. Then (3) vanishes for two distinct values of λ/μ in F. Hence the family contains two distinct forms each a multiple of a perfect square. Thus by a linear transformation in F we may replace the pair (1) by a pair

$$q_1 = a_0(x^2 + ay^2), \quad q_2 = b_0(x^2 + by^2), \quad a_0 b_0 \neq 0, \quad a \neq b, \tag{27}$$

of resultant $-a_0^2 b_0^2 (a - b)^2$. The first form of an equivalent pair may be taken to be $A_0(X^2 + AY^2)$, where $A = d^2 a$. For $X = \xi$, $Y = \eta/d$,

$$Q_1 = A_0(\xi^2 + a\eta^2), \quad Q_2 = B_0(\xi^2 + B\eta^2), \quad A_0 B_0 \neq 0, \quad a \neq B. \tag{28}$$

As shown in § 3, the transformations of q_1 into Q_1 are

$$x = \alpha\xi \mp a\gamma\eta, \quad y = \gamma\xi \pm \alpha\eta, \quad a_0(\alpha^2 + a\gamma^2) = A_0. \tag{29}$$

This will transform q_2 into Q_2 if, and only if,

$$b_0(\alpha^2 + b\gamma^2) = B_0, \quad \alpha\gamma(a - b) = 0, \quad b_0(a^2\gamma^2 + b\alpha^2) = B_0 B.$$

Now $a \neq b$. According as $\gamma = 0$ or $\alpha = 0$, we have

$$B = b, \qquad A_0/a_0 = B_0/b_0 = \text{square in } \mathsf{F} \text{ (viz., } \alpha^2); \tag{30}$$

$$B = a^2/b, \quad A_0/a_0 a = B_0/b_0 b = \text{square in } \mathsf{F} \text{ (viz., } \gamma^2), \quad b \neq 0. \tag{31}$$

For the pair (27), the determinant (3) becomes

$$a_0^2 a \lambda^2 + a_0 b_0 (a + b)\lambda\mu + b_0^2 b \mu^2$$

and vanishes for $\lambda/\mu = -b_0/a_0$, $-bb_0/aa_0$. For (4), the roots are $-B_0/A_0$, $-BB_0/aA_0$. The conditions for the identity of the two sets of roots are (30) or (31), apart from the requirement that the ratios be squares. The latter is

---

* Then $k^2 + 4af^2 = 0$, $k = f = 0$, so that the second form (11) is a multiple of the first. This is evident since the forms have a common root and the first is irreducible.

therefore a condition additional to those in the algebraic theory. For a finite field, it is shown in § 10 that the two pairs of forms are equivalent if their algebraic invariants satisfy (5), and if two modular invariants have equal values.

5. Finally, let q_1 be reducible in the field, the necessary and sufficient condition for which is $-a=$ square or zero. Then q_1 may be given one of the types $2xy$, a_0x^2. By (5), $-A=$ square or zero. After a preliminary transformation we may take Q_1 to be $2xy$ or A_0x^2. Then let q_2 and Q_2 have the coefficients b_i and B_i, respectively.

The automorphs of $2xy$ are $(kx, k^{-1}y)$, $(ky, k^{-1}x)$. Hence must

$$B_1=b_1,\ B_0=k^2b_0,\ B_2=k^{-2}b_2;\ \text{or}\ B_1=b_1,\ B_0=k^{-2}b_2,\ B_2=k^2b_0. \tag{32}$$

Necessary and sufficient conditions for equivalence are that $B_1=b_1$, $B_0B_2=b_0b_2$ (to which (5) now reduce), and that if $b_i\neq 0$ ($i=0$ or 2) one of the ratios of B_0, B_2 to b_i shall be a square $\neq 0$ in the field; while if $b_0=b_2=0$, then* $B_0=B_2=0$. For a finite field the last conditions may be expressed by a modular invariant (§ 11).

6. For $q_1=a_0x^2$, $Q_1=A_0x^2$, a necessary condition for equivalence is $A_0=t^2a_0$. The general transformation of the first pair into the second is then $(tx,\ rx+sy)$, where

$$B_0=b_0t^2+2b_1rt+b_2r^2,\quad B_1=b_1st+b_2rs,\quad B_2=b_2s^2. \tag{33}$$

For $a_1=a_2=0$, conditions (5) reduce to $A_0B_2:a_0b_2=B:b=$ square. These, with $A_0/a_0=$ square, are sufficient if $b_2\neq 0$ or if $b_2=0$, $b_1\neq 0$ (whence $B_2=0$, $B_1\neq 0$), since $A_0=t^2a_0$ and (33) may then be satisfied by choice of t, s, r in the field. The condition $A_0/a_0=$ square may be expressed in a finite field by the modular invariant Q_a (§ 12). If† $b_1=b_2=0$, (5) give $B_1=B_2=0$; further necessary conditions are $B_0:b_0=A_0:a_0=$ square (viz., t^2). For a finite field the latter conditions may be expressed by the modular invariants Q_a and K_1 (§ 12).

7. Every binary linear homogeneous transformations with coefficients in a given field can be generated by the three types

$$x=x'+ty',\quad y=y'; \tag{34}$$
$$x=y',\quad y=-x'; \tag{35}$$
$$x=x',\quad y=\lambda y'; \tag{36}$$

* For $q_1=Q_1=2xy$, $q_2=2b_1xy$, $Q_2=B_0x^2+2b_1xy+B_2y^2$, the minors of $|\lambda q_1+\mu q_2|$ have the factor $\lambda+\mu b_1$. Those of $|\lambda Q_1+\mu Q_2|$ have the same factor if and only if $B_0=B_2=0$. See § 1.

† Then $q_1=a_0x^2$, $q_2=b_0x^2$, and the minors of $|\lambda q_1+\mu q_2|$ have the factor $\lambda a_0+\mu b_0$. For a second pair of such forms, the factor is $\lambda A_0+\mu B_0$. The relative invariance of this factor leads to the condition $B_0:b_0=A_0:a_0$. See § 1.

where t and λ are arbitrary non-vanishing elements of the field. Under these transformations the forms (1) become q_1', q_2', with the coefficients

$$\left.\begin{array}{lll} a_0' = a_0, & a_1' = a_1 + t\,a_0, & a_2' = a_2 + 2\,t\,a_1 + t^2 a_0, \\ b_0' = b_0, & b_1' = b_1 + t\,b_0, & b_2' = b_2 + 2\,t\,b_1 + t^2 b_0; \end{array}\right\} \quad (37)$$

$$a_0' = a_2, \quad a_1' = -a_1, \quad a_2' = a_0, \quad b_0' = b_2, \quad b_1' = -b_1, \quad b_2' = b_0; \qquad (38)$$

$$a_i' = \lambda^i a_i, \quad b_i' = \lambda^i b_i \qquad (i = 0, 1, 2). \qquad (39)$$

Let the field be the Galois field $GF[p^n]$ of order p^n, $p > 2$. Set

$$\tau = \tfrac{1}{2}(p^n - 1). \qquad (40)$$

If C denotes a binomial coefficient, we have

$$C_i^{2\tau} \equiv (-1)^i, \quad (k - l)^{2\tau} \equiv \sum_{i=0}^{2\tau} k^i l^{2\tau - i} \qquad (\text{mod } p). \qquad (41)$$

For the invariant $a = a_0 a_2 - a_1^2$ of q_1, we have

$$a^{2\tau} \equiv \sum_{i=0}^{\tau-1} a_0^i a_2^i a_1^{4\tau - 2i} + \sum_{j=\tau}^{2\tau} a_0^j a_2^j a_1^{4\tau - 2j}.$$

To the first sum we apply

$$a_1^{2\tau + r} = a_1^r \qquad (r > 0). \qquad (42)$$

In the last sum we set $j = \tau + i$. Hence

$$a^{2\tau} - 1 = (a_0^\tau a_2^\tau + 1)\,\sigma, \quad \sigma \equiv \sum_{i=0}^{\tau} a_0^i a_2^i a_1^{2\tau - 2i} - 1. \qquad (43)$$

We may now show that q_1 has the absolute invariant

$$Q = (a_0^\tau + a_2^\tau)\,\sigma. \qquad (44)$$

Obviously Q is absolutely invariant under (38) and (39). It remains to establish its invariance under (37). Let the latter give to a_2^τ and σ the increments δ and σ_1. Then the increments to $a^{2\tau} - 1$ and Q are

$$(a_0^\tau a_2^\tau + 1)\,\sigma_1 + a_0^\tau \delta\,(\sigma + \sigma_1) = 0, \qquad (a_0^\tau + a_2^\tau)\,\sigma_1 + \delta\,(\sigma + \sigma_1).$$

If $a_0 \neq 0$, we multiply the former by a_0^τ and obtain the latter, since $a_0^{2\tau} = 1$. If $a_0 = 0$, then $\sigma = a_1^{2\tau} - 1$, $a_1 \sigma = 0$, so that Q is unaltered by $a_2' = a_2 + 2\,t\,a_1$.

Since $a_i\,(a_i^{2\tau} - 1) = 0$ in the field, we have by (43), (44),

$$(a^{2\tau} - 1)^2 - Q^2 = (a_0^{2\tau} - 1)(a_2^{2\tau} - 1)\,\sigma^2 = (a_0^{2\tau} - 1)(a_2^{2\tau} - 1)(a_1^{2\tau} - 1)^2.$$

But $(k^{2\tau} - 1)^2 = -(k^{2\tau} - 1)$. Hence*

$$a^{2\tau} - 1 + Q^2 = I = (a_0^{2\tau} - 1)(a_1^{2\tau} - 1)(a_2^{2\tau} - 1). \qquad (45)$$

---

* Concerning invariant I, see *Trans. Amer. Math. Soc.*, Vol. VIII (1907), p. 206.

Multiplying this by a and applying the obvious relation $aI = 0$, we get $aQ^2 = 0$. Hence $aQ = 0$.

A complete set* of independent invariants of q_1 is given by a and Q. Let ν be a fixed not-square. Then q_1 can be reduced by a linear transformation in the $GF[p^n]$, $p > 2$, to one and but one of the forms

$$\begin{array}{llllll} q_1 = x^2 - \nu y^2, & 2xy, & x^2, & \nu x^2, & \text{Identically zero}; \\ a = -\nu, & -1, & 0, & 0, & 0; \\ Q = 0, & 0, & -1, & +1, & 0. \end{array}$$

Two forms are equivalent if and only if they have the same Q and a^τ.

8. If we replace each a_i by $a_i + kb_i$ in the determinant a of q_1, we obtain $a + k\theta + k^2 b$, where θ is the simultaneous invariant (2) of q_1 and q_2. From Q_a we obtain similarly new simultaneous invariants K_i:

$$Q_{a+kb} = Q_a + k^\tau Q_b + \sum_{i=1}^{2\tau} k^i K_i, \tag{46}$$

the exponents $> 2\tau$ of k having been reduced by $k^{2\tau+r} = k^r$. We shall be able to apply the invariants K_i without obtaining their explicit expressions.

For the case $p^n = 3$, we have

$$\left.\begin{array}{l} K_1 = a_0^2 b_2 + a_2^2 b_0 + a_1^2 b_2 + a_1^2 b_0 - a_0 a_2 b_2 - a_0 a_2 b_0 - a_0 a_1 b_1 - a_1 a_2 b_1, \\ K_2 = b_0^2 a_2 + b_2^2 a_0 + b_1^2 a_2 + b_1^2 a_0 - b_0 b_2 a_2 - b_0 b_2 a_0 - b_0 b_1 a_1 - b_1 b_2 a_1, \end{array}\right\} \tag{47}$$

K_1 and K_2 being interchanged when the a's and b's are interchanged.

9. We may now readily derive a complete set of non-equivalent canonical types of a pair of binary quadratic forms in the $GF[p^n]$, $p > 2$, the various types being invariantly characterized. We begin with the case in which q_1 is irreducible in the field, while the resultant R, given by (25), is zero or the negative of a not-square. By § 3, we may take $q_1 = x^2 - \nu y^2$, ν being a fixed not-square; $q_2 = mq_1$ if $R = 0$; $q_2 = ex^2 + 2fxy + gy^2$ if $-R$ is a not-square, where, for arbitrary elements b and θ for which $\theta^2 + 4\nu b$ is a not-square $(-R)$, e, f, g is a particular set of solutions of $eg - f^2 = b$, $g - \nu e = \theta$. Thus e is a fixed element for which $\lambda \equiv e(\theta + \nu e) - b$ is a square, f is a fixed square root of λ, while $g = \theta + \nu e$. In either case, two such pairs of forms are equivalent only if they have equal values of the invariants b, θ (since the a's are equal).

10. Next, let q_1 be irreducible, and $-R$ be a square $\neq 0$. In (27), (28), we may set $a = -\nu$, $a_0 = 1$ or ν, $A_0 = 1$ or ν. Conditions (30) apply only

* For proof in special fields see *ibid.*, §§ 8, 13.

when A_0/a_0 is a square (whence $A_0 = a_0$) and are then trivial. Hence equivalence arises only when (31) can be satisfied. For $b = 0$, the canonical types are

$$q_1 = a_0(x^2 - \nu y^2), \quad q_2 = b_0 x^2 \quad (a_0 = 1 \text{ or } \nu,\ b_0 \neq 0). \tag{48}$$

Consider (31) for $b \neq 0$, $a = -\nu$. If -1 is a not-square, A_0/a_0 must be a square, whence $A_0 = a_0$, $B_0 = -b_0 b/\nu$, $B = \nu^2/b$; the canonical types are

$$q_1 = a_0(x^2 - \nu y^2), \quad q_2 = b_0(x^2 + by^2)\ (a_0 = 1 \text{ or } \nu,\ b_0 \neq 0,\ b \neq 0, -\nu), \tag{49}$$

only one of each pair (b_0, b), $(-b_0 b/\nu, \nu^2/b)$ being retained.*

If -1 is a square, (31) requires that A_0/a_0 be a not-square. Taking $a_0 = 1$, $A_0 = \nu$, we have $B_0 = -b_0 b$, $B = \nu^2/b$; for these values (27) and (28) are equivalent. Hence for -1 a square, the canonical types are

$$q_1 = x^2 - \nu y^2, \quad q_2 = b_0(x^2 + by^2) \quad (b_0 \neq 0,\ b \neq 0, -\nu), \tag{50}$$

and no two such pairs are equivalent. However, the pair (50) has the same determinants and the same value of θ as the similar pair with $B_0 = -b_0 b/\nu$, $B = \nu^2/b$, but not for any further pairs. Hence new invariants are required to distinguish two such pairs. Similar remarks apply to (48) and to (49).

To this end we determine the value of the absolute invariants $K_{2\tau}$ and† K_1, defined by (46), for the case $a_1 = b_1 = 0$. Then Q_{a+kb} becomes

$$Q'_{a+kb} = F_{02} + F_{20}, \quad F_{02} = (a_0 + kb_0)^{2\tau}(a_2 + kb_2)^\tau - (a_0 + kb_0)^\tau, \tag{51}$$

F_{20} being derived from F_{02} by interchanging a_0 with a_2 and b_0 with b_2. By (41),

$$(a_0 + kb_0)^{2\tau} \equiv \sum_{i=0}^{2\tau} (-1)^i k^i b_0^i a_0^{2\tau - i}.$$

The coefficient of $k^{2\tau}$ in F_{02} is therefore ‡

$$\sum_{j=0}^{\tau} [c_j^\tau b_2^j a_2^{\tau-j}]\,[(-1)^{2\tau-j} b_0^{2\tau-j} a_0^j].$$

Applying (02) to the subscripts, we obtain the required terms in F_{20}. Set $a_2 = a_0 a$, $b_2 = b_0 b$, as in (27). Then the terms free of a_1, b_1 in $K_{2\tau}$ are

$$K'_{2\tau} = a_0^\tau b_0^{2\tau} \sum_{j=0}^{\tau} (-1)^j c_j^\tau (a^{\tau-j} b^j + a^j b^{2\tau-j}).$$

---

* For example, if b is a not-square, we may restrict b_0 to the squares; if b is a square it may be restricted to the squares β for which the pairs $(\beta, \nu^2/\beta)$ yield all the squares $\neq 0, -\nu$,

† In §11 we employ K_τ. But for $a_1 = b_1 = 0$, $K_\tau = a_0^{2\tau} b_0^\tau [a^\tau + (-1)^\tau] (a - b)^\tau = 0$, since $(-a)^\tau + 1$ equals $\nu^\tau + 1 = 0$.

‡ There are no further terms in $k^{2\tau}$ obtained from $k^{4\tau} = k^{2\tau}$, etc.

In the first sum replace j by $\tau - j$, and hence $\tau - j$ by j. Thus, for $b_0 \neq 0$,

$$K'_{2\tau} = a_0^\tau [(-1)^\tau + b^\tau] [\sum_{j=0}^{\tau} (-1)^j c_j^\tau a^j b^{\tau-j}] = a_0^\tau [(-1)^\tau + b^\tau] (b-a)^\tau. \quad (52)$$

The sum of the coefficients of k and $k^{2\tau+1} \equiv k$ in F_{02} is

$$\tau a_0^{2\tau} a_2^{\tau-1} b_2 + 2\tau a_0^{2\tau-1} b_0 a_2^\tau - \tau a_0^{\tau-1} b_0 + \sum_{j=1}^{\tau} c_j^\tau b_2^j a_2^{\tau-j} (-1)^{1-j} b_0^{2\tau+1-j} a_0^{j-1}.$$

Replace a_2 by $a_0 a$, b_2 by $b_0 b$. Let $p^n > 3$, so that $\tau > 1$, $a_0^{3\tau-1} = a_0^{\tau-1}$. Then the terms free of a_1, b_1 in K_1 are

$$K'_1 = a_0^{\tau-1} b_0 \{\tau a^{2\tau} - \tau - a^{2\tau-1} b - a^\tau + \sum_{j=1}^{\tau} (-1)^{1-j} c_j^\tau (a^{\tau-j} b^j + a^{j-1} b^{2\tau+1-j})\}.$$

In the final terms of the sum replace j by $\tau + 1 - j$. There results

$$\sum_{j=1}^{\tau} (-1)^{\tau-j} c_{j-1}^\tau a^{\tau-j} b^{\tau+j}.$$

We shall employ K'_1 only for $a \neq 0$, $b^\tau = (-1)^{\tau+1}$. Then

$$K'_1 = a_0^{\tau-1} b_0 \{-a^{-1} b - a^\tau + \sum_{j=1}^{\tau} (-1)^{1-j} (c_j^\tau + c_{j-1}^\tau) a^{\tau-j} b^j\}.$$

Since $c_j^\tau + c_{j-1}^\tau = c_j^{\tau+1}$, we have

$$K'_1 = -a_0^{\tau-1} b_0 a^{-1} (a-b)^{\tau+1}, \text{ if } b^\tau = (-1)^{\tau+1}, \ \tau > 1. \quad (53)$$

For the forms (48), $K_{2\tau} = -(-1)^\tau a_0^\tau$, by (52), so that a_0^τ and hence also a_0 is absolutely invariant. Thus $|q_1| = -a_0^2 \nu$ is invariant. Then by (5), $\theta = -a_0 b_0 \nu$ and hence also b_0 is absolutely invariant. Thus $K_{2\tau}$, a and θ differentiate the forms (48).

For (49) we have -1 a not-square. We set $\nu = -1$. Then

$$|q_1| = a_0^2 = 1, \quad |q_2| = b_0^2 b, \quad \theta = a_0 b_0 (b+1).$$

For such pairs of forms, the above are absolute invariants. From

$$A_0 = \pm a_0, \quad B_0^2 B = b_0^2 b, \quad A_0 B_0 (B+1) = a_0 b_0 (b+1),$$

we obtain, by eliminating B and A_0,

$$(B_0 \mp b_0)(b_0 b / B_0 \mp 1) = 0.$$

We need only examine the sets $(\pm b_0, b)$, since the other sets $(\pm b_0 b, 1/b)$ are not retained in the types (49). By (52), (53),

$$K_{2\tau} = a_0^\tau (b^\tau - 1)(b+\nu)^\tau; \quad K_1 = a_0^{\tau-1} b_0 \nu^{-1} (b+\nu)^{\tau+1} \text{ if } b^\tau = 1,$$

since τ is odd and > 1 for b a square ($b \neq 0$, $-\nu$ implies $b = \nu$ when $p^n = 3$).

When a_0 and b_0 are changed in sign, so also are $K_{2\tau}$ and K_1, and at least one is not zero for each $b \neq 0$. Hence the invariants differentiate the forms (49).

Finally, for (50) we have -1 a square, τ even. Then

$$K_{2\tau} = (b^\tau + 1)(b + \nu)^\tau; \quad K_1 = -\nu^{-1} b_0 (b + \nu)^{\tau+1} \text{ if } b^\tau = -1.$$

Each is changed in sign when b_0 is replaced by $-b_0 b/\nu$, and b by ν^2/b. Hence the invariants a, b, θ, $K_{2\tau}$, K_1 differentiate the forms (50).

11. To differentiate pairs of forms of which q_1 is $2xy$, we employ K_τ, defined by (46), for $a_0 = a_2 = 0$, $a_1 = 1$. Then Q_{a+kb} becomes

$$k^\tau (b_0^\tau + b_2^\tau) \{-1 + \sum_{i=0}^{\tau} k^{2i} b_0^i b_2^i (1 + k b_1)^{2\tau - 2i}\}.$$

Since the constant terms within the brackets cancel, terms in $k^\tau = k^{3\tau}$ are obtained only by employing the term of highest degree in the final binomial. Hence the coefficient of $k^{3\tau}$ is

$$(b_0^\tau + b_2^\tau) \sum_{i=0}^{\tau} b_0^i b_2^i b_1^{2\tau - 2i}.$$

This must equal $Q_b + K_\tau''$, where K_τ'' is the value of K_τ for $a_0 = a_2 = 0$, $a_1 = 1$. Hence, by (44),

$$K_\tau'' = b_0^\tau + b_2^\tau.$$

Hence to the conditions $B_1 = b_2$, $B_0 B_2 = b_0 b_2$ in § 5 for the equivalence of $2xy$, q_2 with $2xy$, Q_2, we may add $B_0^\tau + B_2^\tau = b_0^\tau + b_2^\tau$. From the latter and $B_0^\tau B_2^\tau = b_0^\tau b_2^\tau$, we find that B_0^τ, B_2^τ must equal, in some order, b_0^τ, b_2^τ. Hence the algebraic invariants a, b, θ and the modular invariant K_τ fully differentiate all pairs of forms of which the first is reducible, but not a multiple of a perfect square.

For a complete set of canonical types in which $q_1 = 2xy$, we may give q_2 the forms in the following table, which shows the values of the above invariants:

q_2	$\lvert q_2 \rvert$	θ	K_τ
$2b_1 xy$	$-b_1^2$	$-2b_1$	0
$\mu x^2 + 2b_1 xy \quad (\mu = 1 \text{ or } \nu)$	$-b_1^2$	$-2b_1$	μ^τ
$x^2 + 2b_1 xy + b_2 y^2 \quad (b_2 \neq 0)$	$b_2 - b_1^2$	$-2b_1$	$1 + b_2^\tau$
$\nu x^2 + 2b_1 xy + \nu c^2 y^2 \quad (c \neq 0)$	$\nu^2 c^2 - b_1^2$	$-2b_1$	-2

where b_1, b_2, c are arbitrary, while ν is a fixed not-square. Obviously these pairs are differentiated by the given invariants, necessarily absolute in view of q_1.

12. Finally, for $q_1 = a_0 x^2$, $q_2 = b_0 x^2$, the theory in § 6 is readily completed invariantively for a finite field. In view of the absolute invariants

$$Q_a = -a_0^\tau, \quad K_1 = -\tau a_0^{\tau-1} b_0,$$

necessary conditions for equivalence are $A_0^\tau = a_0^\tau$, $A_0^{\tau-1} B_0 = a_0^{\tau-1} b_0$. Multiplying the latter by $A_0 a_0$ and applying the former, we get $a_0 B_0 = A_0 b_0$. Hence $B_0 : b_0 = A_0 : a_0 =$ square. These, together with conditions (5) on the algebraic invariants a, b, θ, were shown to be sufficient conditions for the equivalence of two such pairs of forms.

As canonical types, when $q_1 = a_0 x^2$, we may take

$$q_1 = a_0 x^2 \,(a_0 = 1 \text{ or } \nu), \qquad q_2 = b_0 x^2 + b_2 y^2 \,(b_2 = 1 \text{ or } \nu), \qquad 2xy, \text{ or } b_0 x^2.$$

For $q_1 \equiv 0$, the canonical forms of q_2 are given by § 7.

13. As a partial summary of our results, we may state the

THEOREM. *Within a finite field of order p^n, $p > 2$, two pairs of binary quadratic forms are equivalent under linear transformation if, and only if, the algebraic invariants a, b, θ of the one pair equal the products of those of the other pair by the same square and the (absolute) modular invariants Q_a, K_1, K_τ, $K_{2\tau}$ have the same values for the two pairs of forms.**

REDUCTION OF TWO QUADRATIC FORMS IN THE $GF[2^n]$; THEIR INVARIANTS.

14. Consider two quadratic forms with coefficients in the $GF[2^n]$,

$$q_1 = a_0 x^2 + a_1 xy + a_2 y^2, \quad q_2 = b_0 x^2 + b_1 xy + b_2 y^2. \tag{54}$$

Under transformation (34), these become forms with the coefficients

$$a_2' = a_2 + ta_1 + t^2 a_0, \quad b_2' = b_2 + tb_1 + t^2 b_0, \quad a_i' = a_i, \; b_i' = b_i \quad (i = 0, 1). \tag{55}$$

Transformation (35), which now merely interchanges x and y, gives rise to

$$(a_0 a_2)\,(b_0 b_2). \tag{56}$$

Obvious (relative) invariants are a_1, b_1 and the resultant

$$R = a_2^2 b_0^2 + b_2^2 a_0^2 + a_2 (a_0 b_1^2 + a_1 b_0 b_1) + b_2 (a_1^2 b_0 + a_0 a_1 b_1). \tag{57}$$

15. We are led naturally to an important invariant (58) of a quadratic

---

* These seven invariants do not, however, form a complete system; there exist invariants of odd weights I hope to take up this problem on another occasion. For $p = 2$, see §§ 31–35.

form q_1 by determining the necessary and sufficient condition for its irreducibility. First, let q_1 be irreducible in the $GF[2^n]$; then each $a_i \neq 0$. For

$$x = a_0^{-1/2} X, \quad y = a_0^{1/2} a_1^{-1} Y,$$

we have

$$q_1 = X^2 + XY + \gamma Y^2, \quad \gamma = a_0 a_2 / a_1^2 = a_0 a_2 a_1^{2^n - 3} \text{ or } a_0 a_2 a_1,$$

according as $n > 1$ or $n = 1$. Let $X = \xi + t\eta$, $Y = \eta$. Then

$$q_1 = \xi^2 + \xi\eta + c\eta^2, \quad c = t^2 + t + \gamma.$$

The latter is solvable for t in the $GF[2^n]$ if, and only if

$$\chi(c) = \chi(\gamma), \quad \text{where} \quad \chi(s) = \sum_{i=0}^{n-1} s^{2^i}.$$

If $\chi(\gamma) = 0$, we could choose t to make $c = 0$, contrary to the irreducibility of q_1. But $\chi^2 = \chi$. Hence a necessary condition for the irreducibility of q_1 is $\chi(\gamma) = 1$. The condition is also sufficient; for, if q_1 vanishes for $X = rY$, r in the $GF[2^n]$, then $r^2 + r \equiv \gamma$, so that $\chi(\gamma) = 0$. *Hence $a_0 x^2 + a_1 xy + a_2 y^2$ is irreducible in the $GF[2^n]$ if, and only if, $H_a = 1$, where*

$$H_a = \sum_{i=0}^{n-1} (a_0 a_1^{2^n - 3} a_2)^{2^i} \text{ if } n > 1, \quad H_a = a_0 a_1 a_2 \text{ if } n = 1. \tag{58}$$

This function is unaltered by transformations (39) and (56). We next show that it is unaltered by (55). If $n = 1$, then $t^2 \equiv t$, so that the increment to H_a under (55) is $t a_0 a_1 (a_1 + a_0) \equiv 0$. Next, let $n > 1$. Since

$$(r + s)^{2^i} \equiv r^{2^i} + s^{2^i} \pmod{2},$$

the increment to H_a is

$$\sum_{i=0}^{n-1} a_0^{2^i} a_1^{2^i(2^n - 2)} t^{2^i} + \sum_{i=0}^{n-1} a_0^{2^{i+1}} a_1^{2^i(2^n - 3)} t^{2^{i+1}}.$$

In the first sum the term given by $i = 0$ may be replaced by the summand for $i = n$. In the new first sum we replace i by $i + 1$ and obtain the second sum, since the exponent $2^{i+1}(2^n - 2)$ of a_1 may be replaced by $2^i(2^n - 1 + 2^n - 3)$ and hence by $2^i(2^n - 3)$. *Hence* H_a is an absolute invariant of q_1 in the $GF[2^n]$.*

A further absolute invariant of q_1 analogous to (45), is

$$I_a = (a_0^m - 1)(a_1^m - 1)(a_2^m - 1) \quad (m = 2^n - 1). \tag{59}$$

The invariants a_1, H_a, I_a of q_1 are independent† (§ 20).

---

* Cf. *Transactions*, l. c., pp. 213–214.

† Cf. *ibid*, § 28; in the second table of § 26, K is a misprint for χ.

16. To obtain simultaneous invariants of the pair (54), we replace each a_i by $a_i + kb_i$ in an invariant of q_1. Those obtained from H_a are functions of a_1, b_1, H_a, H_b, R (§ 30). For I_a, we set

$$I_{a+kb} = I_a + \sum_{r=1}^{m} k^r V_r. \tag{60}$$

We shall study the invariants V_r directly from the preceding definition. We can, however, obtain their explicit expressions, noting that, as in (41), each binomial coefficient C_i^m is odd:

$$V_r = (a_0^m - 1)(a_1^m - 1)\, a_2^{m-r} b_2^r + (a_2^m + b_2^m - 1)\, C_r$$
$$+ \sum_{l=1}^{r=1} a_2^{m-r+l} b_2^{r-l} C_l + \sum_{l=r+1}^{m} a_2^{l-r} b_2^{m-l+r} C_l, \tag{61}$$

$$C_l = (a_0^m - 1)\, a_1^{m-l} b_1^l + (a_1^m + b_1^m - 1)\, a_0^{m-l} b_0^l$$
$$+ \sum_{i=1}^{l-1} a_0^{m-i} b_0^i a_1^{m-l+i} b_1^{l-i} + \sum_{i=l+1}^{m} a_0^{m-i} b_0^i a_1^{i-l} b_1^{m-i+l}. \tag{62}$$

Thus, for $n = 1$,

$$V_1 = (a_0 - 1)(a_1 - 1)\, b_2 + (a_2 + b_2 - 1)(b_0 b_1 + b_0 + b_1 + a_0 b_1 + a_1 b_0). \tag{61'}$$

17. We pass to the reduction of the pair of forms (54), of which q_1 is now assumed to be irreducible in the $GF[2^n]$. Applying the transformations defined at the beginning of § 15, we get

$$q_1 = \xi^2 + \xi\eta + c\eta^2, \quad q_2 = e\xi^2 + f\xi\eta + g\eta^2, \tag{63}$$

where

$$e = b_0/a_0, \quad f = b_1/a_1, \quad g = t^2 b_0/a_0 + t\, b_1/a_1 + b_2 a_0/a_1^2,$$

c being a fixed root of $\chi(c) = 1$, t a root of $t^2 + t + a_0 a_2/a_1^2 = c$. For further reductions we must apply one of the automorphs of (63_1):

$$A: \begin{pmatrix} \alpha & \tau\alpha + c\beta \\ \beta & \alpha + (\tau + 1)\beta \end{pmatrix}, \quad \alpha^2 + \alpha\beta + c\beta^2 = 1;\ \tau = 0 \text{ or } 1.$$

Since $|A| = 1$, A replaces q_2 by a form with the same f. Hence it suffices to normalize

$$q_2 + f q_1 = (r\xi + s\eta)^2, \quad r^2 = e + f, \quad s^2 = g + cf.$$

The eliminant of q_1 and $r\xi + s\eta$ is

$$E_{rs} = s^2 + sr + cr^2.$$

Since E^2 is the resultant of forms (63), E is absolutely invariant under A (a verification is given below). Now A replaces $r\xi + s\eta$ by $\rho\xi + \sigma\eta$,

$$\rho = r\alpha + s\beta, \quad \sigma = (r\tau + s)\alpha + \{ rc + s(\tau + 1) \}\beta.$$

The determinant of the coefficients of α and β equals E_{rs}. Thus

$$\alpha E_{rs} = \rho \{ rc + s(\tau + 1) \} + \sigma s, \quad \beta E_{rs} = \rho(r\tau + s) + \sigma r,$$
$$(\alpha^2 + \alpha\beta + c\beta^2) E_{rs}^2 = E_{rs} E_{\rho\sigma}.$$

Hence if $E_{rs} = E_{\rho\sigma} \neq 0$, there exists a transformation A of determinant unity which replaces $r\xi + s\eta$ by $\rho\xi + \sigma\eta$. Next, $E_{rs} = 0$ implies $r = s = 0$, in view of the irreducibility of q_1. Hence two pairs of forms (63), with the same root c of $\chi(c) = 1$, are equivalent if, and only if, they have the same f and equal resultants. To obtain canonical types, we may set $r = 0$; then $q_2 + fq_1 = E\eta^2$.

It follows* that two pairs (54) having $H_a = 1$ are equivalent if, and only if, the ratios $a_1^4 : b_1^4 : R$ are the same for each pair.

18. The necessary (§ 15) and sufficient conditions that q_1 shall be reducible to $\xi\eta$ are $H_a = 0$, $a_1 \neq 0$. To prove them sufficient, set

$$x = (1 + a_0 k)\xi + k\eta, \quad y = a_1^{-1}(a_0\xi + \eta).$$

Then

$$q_1 = a_0^2 l \xi^2 + \xi\eta + l\eta^2, \quad l = a_0 k^2 + k + a_2/a_1^2.$$

If $H_a = 0$, we can determine k in the $GF[2^n]$ to make $l = 0$. Indeed, if $a_0 = 0$, we take $k = a_2/a_1^2$. If $a_0 \neq 0$, set $t = a_0 k$; then $a_0 l = t^2 + t + a_0 a_2/a_1^2$. Hence, as in § 15, t can be chosen to make $a_0 l = 0$. Under the above transformation,

$$q_2 = B_0\xi^2 + a_1^{-1} b_1 \xi\eta + B_2\eta^2, \quad B_2 = b_0 k^2 + a_1^{-1} b_1 k + a_1^{-2} b_2, \quad B_0 = a_0^2 B_2 + b_0 + a_1^{-1} a_0 b_1.$$

The resultant of $\xi\eta$ and q_2 is $R = B_0 B_2$. If $B_0 \neq 0$, we multiply ξ by $B_0^{-1/2}$, η by $B_0^{1/2}$ and obtain

$$q_1 = \xi\eta, \quad q_2 = \xi^2 + a_1^{-1} b_1 \xi\eta + R\eta^2.$$

The case $B_0 = 0$, $B_2 \neq 0$, is reduced to the preceding by interchanging ξ and η. Finally, let $B_0 = B_2 = 0$, necessary and sufficient conditions for which are $b_0 = a_1^{-1} a_0 b_1$, $b_2 = a_1^{-1} a_2 b_1$, as is directly evident or as may be verified by eliminating k between $l = 0$, $B_2 = 0$. Then $q_2 = a_1^{-1} b_1 q_1$.

The two canonical types obtained when $R = 0$ may be differentiated by the absolute invariant V_1. For $a_0 = a_2 = 0$, $a_1 = 1$,

$$V_1 = b_1 (b_0^m - 1)(b_2^m - 1),$$

by § 21. If $b_0 = b_2 = 0$, $V_1 = b_1$; if $b_0 \neq 0$, $V_1 = 0$. For the special case $b_1 = 0$, we distinguish the pairs by the invariant I_b.

---

* The transformation used to reduce (54) to (63) was of determinant $1/a_1$. Hence the resultant E^2 of (63) equals $1/a_1^4$ times the resultant R of (54). It is not difficult to verify this directly, employing the above values of e, f, g, r, s.

19. Next, q_1 is reducible to ξ^2 if, and only if, $a_1 = 0$, $I_a = 0$, the latter showing that a_0 and a_2 are not both zero. To avoid a separation into cases, we apply the transformation

$$\xi = a_0^{2^{n-1}} x + a_2^{2^{n-1}} y, \quad \eta = a_2^{2^{n-1}-1} x + a_0^{2^{n-1}-1} (a_2^{2^n-1} - 1) y,$$

of determinant $a_0^m (a_2^m - 1) - a_2^m = 1$, by $I_a = 0$. Solving, we get

$$x = a_0^{2^{n-1}-1} (a_2^{2^n-1} - 1) \xi + a_2^{2^{n-1}} \eta, \quad y = a_2^{2^{n-1}-1} \xi + a_0^{2^{n-1}} \eta.$$

Hence

$$q_1 = \xi^2, \quad q_2 = \beta_0 \xi^2 + b_1 \xi \eta + \beta_2 \eta^2, \quad \beta_2^2 = R.$$

For $\xi = X$, $\eta = lX + kY\ (k \neq 0)$, we get

$$q_1 = X^2, \quad q_2 = BX^2 + kb_1 XY + k^2 R^{1/2} Y^2, \quad B \equiv \beta_0 + b_1 l + R^{1/2} l^2.$$

If $b_1 \neq 0$, $R = 0$, we take $l = \beta_0/b_1$, $k = 1/b_1$, and have $q_2 = XY$.
If $b_1 = 0$, $R \neq 0$, we take $l = \beta_0^{1/2} R^{-1/4}$, $k = R^{-1/4}$, and have $q_2 = Y^2$.
If $b_1 \neq 0$, $R \neq 0$, set $\rho = R^{1/2}/b_1^2$, and take $k = 1/b_1$. Then

$$q_2 = BX^2 + XY + \rho Y^2, \quad \rho B = \rho \beta_0 + \rho b_1 l + (\rho b_1 l)^2, \quad \chi(\rho B) = \chi(\rho \beta_0).$$

According as $\chi(\rho \beta_0) = 0$ or 1, we may take $B = 0$ or a fixed root of $\chi(B\rho) = 1$. For q_2, H_b is $\chi(B\rho)$, so that the two cases are distinguished by the invariant H_b.

If $b_1 = R = 0$, the types $q_1 = X^2$, $q_2 = BX^2$, are differentiated by the invariant $V_1 = B$. In fact, by § 21, for $a_0 = 1$, $a_1 = a_2 = 0$,

$$V_1 = b_0 (b_1^m - 1)(b_2^m - 1).$$

20. Finally, q_1 vanishes identically if, and only if, $I_a = 1$. As to q_2, we note that the types for a single form have been distinguished invariantively in § 15, and in the opening lines of §§ 18–20. This fact is shown in the following table, which is given primarily for convenience in the computations below:

Case	Coefficients	a_1	I_a	H_a
A	$\begin{cases} a_0 = a_1 = 1, & a_2 = c, \quad \chi(c) = 1, \\ b_0 = b_1 = f, & b_2 = e + cf \end{cases}$	1	0	1
B	$a_0 = a_2 = 0, \quad a_1 = 1$	1	0	0
C	$a_0 = 1, \quad a_1 = a_2 = 0$	0	0	0
D	$a_0 = a_1 = a_2 = 0$	0	1	0

An inspection of the table shows that the invariants are independent: no one is a rational integral function of the other two (§ 23).

21. For each case A, .., D, we shall determine the value of I_{a+kb} from the definition* (59) and then compare the result with (60) to determine the value of V_r. We consider the simplest case first. For the binomial expansions, see (41).

$$\text{(D)}\quad I_{kb}=1+k^m(I_b+1);\quad V_r=0\ (r<m),\quad V_m=I_b+1.$$

$$\text{(C)}\quad I=(\sum_{r=1}^{m}k^r b_0^r)(k^m b_1^m-1)(k^m b_2^m-1)=\sum_{r=1}^{m}k^r b_0^r(b_1^m-1)(b_2^m-1),$$
$$V_r=b_0^r(b_1^m-1)(b_2^m-1).$$

$$\text{(B)}\quad I=(\sum_{r=1}^{m}k^r b_1^r)(k^m b_0^m-1)(k^m b_2^m-1),\quad V_r=b_1^r(b_0^m-1)(b_2^m-1).$$

$$\begin{aligned}\text{(A)}\quad I&=[(1+kf)^m-1]^2[\{ke+c(1+kf)\}^m-1]\\&=[(1+kf)^m-1][k^m e^m-1],\ \text{since } (s^m-1)s=0,\\&=(\sum_{r=1}^{m}k^r f^r)(k^m e^m-1)=\sum_{r=1}^{m}k^r f^r(e^m-1),\quad V_r=f^r(e^m-1).\end{aligned}$$

In case (D), $V_1=0$ if $n>1$, $V_1=I_b+1$ if $n=1$ $(m=2^n-1)$. The properties of V_1 are essentially different in the cases $n>1$, $n=1$; likewise the relations between V_1 and the earlier invariants. This difficulty would be largely obviated by the use of V_m in place of V_1 as the fundamental new invariant. While V_m (like V_1) serves with the earlier invariants to completely characterize the various types of two quadratic forms (§ 23, Note), V_m does not, for $n>1$ form with those invariants a complete set of independent invariants (§ 29), whereas V_1 is found to possess this important property. Since it is essential to preserve V_1 if $n>1$, we shall to replace V_1 when $n=1$ by a modified form Z_1, such that V_1 $(n>1)$ and Z_1 have similar properties.

It will be seen that there results complete uniformity for every n in the, properties of the new invariant replacing V_1, its relations with the invariants a_1, H_a, .., and with the V_r, if we set

$$Z_r=V_r\ (r<m),\quad Z_m=V_m+I_a(I_b+1),\tag{64}$$

for every n. For $n=1$ (61′) gives

$$\begin{aligned}Z_1=&\,a_2b_2(a_0+1)(a_1+1)(b_0+1)(b_1+1)\\&+(a_2+b_2+1)\{(a_0a_1+a_0+a_1)(b_0b_1+b_0+b_1)+a_0b_1+a_1b_0\}.\end{aligned}\tag{64′}$$

* We may also use (61)–(62). In case (A), each $C_l=f^l$.

The above results and those for I_a in § 20 give

$$\left.\begin{array}{l}\text{(A) } Z_r = f^r(e^m - 1);\ \text{(B) } Z_r = b_1^r(b_0^m - 1)(b_2^m - 1);\\ \text{(C) } Z_r = b_0^r(b_1^m - 1)(b_2^m - 1);\ \text{(D) } Z_r = 0\end{array}\right\}(r = 1,\dots,m). \tag{65}$$

Since $\sigma^2 \equiv \sigma$, $\sigma^r \equiv \sigma$ if $\sigma = s^m - 1$, we have*

$$Z_r = Z_1^r \tag{66}$$

for every set of values of the a_i in the field. Hence (66) is a formal equality.

The importance of Z_1 lies in the following interpretation. If q_1 is not identically zero, $Z_1 = t$ if $q_2 \equiv tq_1$, $Z_1 = 0$ if q_2/q_1 is not a constant. If $q_1 \equiv 0$, then $Z_1 = 0$.

22. The following table gives a complete set of non-equivalent canonical types (§§ 17–20) of pairs of quadratic forms in the $GF[2^n]$, and the values for each pair of a set of invariants completely characterizing the types:

	q_1	q_2	a_1	b_1	I_a	I_b	H_a	H_b	R	Z_1
I	$x^2+xy+cy^2$	$fx^2+fxy+(e+cf)y^2$	1	f	0	π	1	χ_1	e^2	$f(e^m-1)$
II	xy	$x^2+fxy+Ry^2$	1	f	0	0	0	χ_2	R	0
III	xy	fxy	1	f	0	f^m-1	0	0	0	f
IV	x^2	$Bx^2+xy+\rho y^2$	0	1	0	0	0	1	ρ^2	0
V	x^2	$xy+\sigma y^2$	0	1	0	0	0	0	σ^2	0
VI	x^2	y^2	0	0	0	0	0	0	1	0
VII	x^2	b_0x^2	0	0	0	b_0^m-1	0	0	0	b_0
VIII	0	$x^2+xy+cy^2$	0	1	1	0	0	1	0	0
IX	0	xy	0	1	1	0	0	0	0	0
X	0	x^2	0	0	1	0	0	0	0	0
XI	0	0	0	0	1	1	0	0	0	0

Here $\chi(s) = \sum_{i=0}^{n-1} s^{2^i}$, $m = 2^n - 1$, c and B are particular solutions of $\chi(c) = 1$, $\chi(B\rho) = 1$, while $\rho \neq 0$. In the following abbreviations

$$\pi = (f^m - 1)(e^m - 1), \quad \chi_1 = f^m + \chi(f^{2^n-2}e), \quad \chi_2 = \chi(f^{2n-3}R), \tag{67}$$

the exponents are to be replaced by unity when $n = 1$.

---

* Special cases may be seen by inspection from (60), since $I^2 \equiv I$. Thus

$$V_r^2 = V_{2r},\ V_{2^{n-1}+\rho}^2 = V_{2\rho+1}\ (\rho = 0;\ r, \rho = 1, 2, \dots, 2^{n-1} - 1).$$

The same relations hold between the C's in (62). In fact, a_2^m enters (61) only with the coefficient C_r; hence the coefficient of a_2^m in V_r^2 is C_r^2.

23. THEOREM. *The invariants a_1, b_1, I_a, I_b, H_a, H_b, R, Z_1 of a pair of quadratic forms in the $GF[2^n]$ are independent: no one is a rational integral function of the others with coefficients in the field.*

To prove that a given invariant is independent of the others, it suffices to specify two pairs of forms for which the given invariant has distinct values, while each of the remaining invariants have the same value for the two pairs of forms. These requirements may be met as follows:

a_1: II, V, $f=1$, $R=\sigma=0$;	H_a: I, III, $e=f=0$;
b_1: V, VI, $\sigma=1$;	H_b: $VIII$, IX;
I_a: VII, XI, $b_0=0$;	R : V, $\sigma=0$, $\sigma=1$;
I_b: II, III, $f=R=0$;	Z_1: II, III, $f=1$, $R=0$.

Note. In view of (66), the proof holds true if we replace Z_1 by any Z_r.

24. Of the preceding eight invariants, a_1, b_1, R are relative, the remaining five absolute. In the proof in § 23, a_1, b_1, R each had the values 0, 1 (and hence their ratio is not a power of the determinant of transformation), when the other seven invariants were equal. Hence all eight invariants are necessary to characterize the canonical forms; in §§ 17–20 they were shown to be sufficient.

THEOREM. *Two pairs of quadratic forms in the $GF[2^n]$ are equivalent if and only if the ratios $a_1^4 : b_1^4 : R$ and the absolute invariants I_a, I_b, H_a, H_b, Z_1 have the same values for each pair of forms.*

25. We shall establish certain important relations between the invariants by verifying the relation for each set of values a_i, b_i defining types I–XI of § 22, and by noting that the relation continues valid when a_1 and b_1 are multiplied by Δ, R by Δ^4, where Δ is any mark $\neq 0$, so that $\Delta^m = 1$. The relation will then be true for every set a_i, b_i in the field and hence be an identity. We begin with

$$\chi[(a_1 b_1)^{2^n-3} R] = a_1^m H_b + b_1^m H_a, \quad H_a(R^m + I_b + 1) = H_b(R^m + I_a + 1), \quad (68)$$

in which $2^n - 3$ is to be replaced by unity if $n = 1$. We have $H_a = 0$ except for I; $a_1 R = a_1 H_b = 0$, except for I and II. Hence proof of (68_1) is needed only for I and II, when it reduces to (67_2), (67_3). Note that $\chi = \chi^2$, so that

$$\chi(f^{2^n-2} e) = \chi(f^{2^n-1+2^n-3} e^2) = \chi(f^{2^n-3} e^2).$$

As to (68_2), $H_a = 0$ except for *I*, $H_b = 0$ except for *I, II, IV, VIII.* Taking these cases in turn, we give the relation to which (68) reduces and then its proof:

(I) $e^m + \pi + 1 = (e^m + 1)\chi_1$; each $= (e^m - 1) f^m$, since $e(e^m - 1) = 0$.

(II) $0 = (R^m + 1)\chi_2$, since $(R^m + 1) R = 0$.

(IV) $0 = \rho^m + 1$, since $\rho \neq 0$.

(VIII) $0 = 1 + 1$ (mod. 2).

By a similar argument we readily prove that

$$Z_1^m = (a_1^m - 1)(b_1^m - 1)\{R^m + (I_a - 1)(I_b - 1)\} + a_1 b_1^{m-1} Z_1, \tag{69}$$

$$I_a Z_1 = I_b Z_1 = R Z_1 = 0, \quad H_a Z_1 = H_b Z_1 = a_1^{m-1} b_1 H_a (R^m - 1). \tag{70}$$

From the definitions of the invariants, we have by inspection

$$a_1 I_a = b_1 I_b = R I_a = R I_b = H_a I_a = H_b I_b = 0, \tag{71}$$

$$a_1^m H_a = H_a = H_a^2, \quad b_1^m H_b = H_b = H_b^2, \quad I_a^2 = I_a, \quad I_b^2 = I_b, \tag{72}$$

while, of course, for any invariant k,

$$k^{m+1} \equiv k^{2^n} = k. \tag{73}$$

26. Other needed relations will be derived from (68)–(73). Multiplying (69) by $b_1 Z_1^s$, we get $b_1 Z_1^s = a_1 b_1^m Z_1^{s+1}$. The case $s = m$ shows that

$$b_1 Z_1^k = a_1^{m+1-k} b_1^k Z_1 \qquad (k = 1, \ldots, m) \tag{74}$$

is true when $k = m$. We prove (74) by induction from k to $k-1$:

$$b_1 Z_1^{k-1} = a_1 b_1^m Z_1^k = a_1^{m+1-(k-1)} b_1^{k-1} Z_1.$$

Similarly, we multiply (69) by $a_1 Z_1^s$ and prove that, if $n > 1$,

$$a_1 Z_1^k = a_1^{m+2-k} b_1^{m+k-1} Z_1 \qquad (k = 1, \ldots, m), \tag{75}$$

in which we may suppress the m in the exponent of b_1 if $k > 1$, that of a_1 if $k = 1$. By (74) and (75) for $k = 1$, we get, if $n > 1$,

$$b_1^m Z_1 = b_1^{m-1}(a_1^m b_1 Z_1) = a_1^m b_1^m Z_1 = a_1^{m-1}(a_1 b_1^m Z_1) = a_1^m Z_1. \tag{76}$$

This result follows at once for any n from the table in § 22. By (73)–(76), every product containing Z_1 and formed from a_1, b_1, Z_1 can be reduced to

$$Z_1^2, \ Z_1^3, \ \ldots, \ Z_1^m, \ a_1^m Z_1, \ a_1^i b_1^j Z_1 \qquad (i, j = 0, 1, \ldots, m-1). \tag{77}$$

27. For $n > 1$, we multiply (68_1) by $a_1 b_1$; then R^{2^i} has the coefficient $(a_1 b_1)^k$, where

$$k = (2^n - 3)\,2^i + 1 = (2^n - 1)(2^i - 1) + 2^n - 2^{i+1},$$

the first part of which may be suppressed by (73) if $i < n - 1$; while if

$i=n-1$, we may reduce k to $2^n-1=m$. We multiply the resulting relation by H_a and apply (72_1), by H_b and apply (72_2), and get

$$b_1^m H_a R^{2^{n-1}} = H_a \sum_{i=0}^{n-2} (a_1 b_1)^{2^n - 2^{i+1}} R^{2^i} + a_1 b_1 H_a + a_1 b_1 H_a H_b, \tag{78}$$

$$a_1^m H_b R^{2^{n-1}} = H_b \Sigma \qquad\qquad + a_1 b_1 H_b + a_1 b_1 H_a H_b. \tag{79}$$

Multiplying (78) by H_b, or (79) by H_a, we get

$$H_a H_b R^{2^{n-1}} = H_a H_b \sum_{i=0}^{n-2} (a_1 b_1)^{2^n - 2^{i+1}} R^{2^i}. \tag{80}$$

28. We proceed to reduce as far as possible the exponent k of R in a product formed from a_1, b_1, H_a, H_b, R, in which initially $k>0$. First, let R^m occur. We first eliminate the terms involving $H_b R^m$ by (68_2). Multiplying the latter by a_1^m, and applying (72_1), (79), we have $H_a R^m$ expressed in terms of R^t ($t<m$). By (68_1), $a_1 b_1 R^m$ is a function of the R^t ($t<m$). Hence the coefficient of R^m may be assumed to be a linear combination of the a_1^i, b_1^i.

Next, consider a product involving R^k ($2^{n-1} \leqq k < m$). By (79), (78), (68_1), (80), a term with a factor $a_1 H_b R^k$, $b_1 H_a R^k$, $a_1 b_1 R^k$, or $H_a H_b R^k$, may be expressed in terms of R^t ($t<k$). Hence the coefficient of R^k may be assumed to be a linear combination of $b_1^i H_b$, $a_1^i H_a$, a_1^i, b_1^i.

Let the same reductions be effected in the terms involving R^m in (69) and (70). In (77), we suppress Z_1^m if $n>1$, but $a_1^m Z_1$ if $n=1$, by means of the reduced form of (69). Employing also (70)–(73), we have at once the following

THEOREM. *Any rational integral function of the invariants*

$$a_1,\ b_1,\ I_a,\ I_b,\ H_a,\ H_b,\ R,\ Z_1 \tag{81}$$

may be reduced by means of relations (68)–(73), *together with* (76) *for* $n=1$, *to a linear function of*

$$\left.\begin{array}{l} I_a I_b,\ a_1^r I_b,\ b_1^r I_a,\ a_1^i H_a I_b,\ b_1^i H_b I_a, \\ a_1^r b_1^s,\ a_1^i b_1^r H_a,\ b_1^i a_1^r H_b,\ a_1^i b_1^j H_a H_b, \\ a_1^r b_1^s R^c,\ a_1^i b_1^r H_a R^c,\ b_1^i a_1^r H_b R^c,\ a_1^i b_1^j H_a H_b R^c \quad (c=1,\ldots,2^{n-1}-1), \\ a_1^r R^d,\ b_1^{i+1} R^d,\ a_1^i H_a R^d,\ b_1^i H_b R^d \quad (d=2^{n-1},\ldots,m-1), \\ a_1^r R^m,\ b_1^{i+1} R^m,\ a_1^i b_1^j Z_1,\ a_1^m Z_1,\ Z_1^2,\ Z_1^3,\ \ldots,\ Z_1^{m-1}, \end{array}\right\} \tag{82}$$

where $r, s = 0, 1, \ldots, m$; $i, j = 0, \ldots, m-1$; $m \equiv 2^n - 1$, *the invariant* $a_1^m Z_1$ *being suppressed if* $n=1$.

For $n=1$, the third and fourth lines of (82) are missing, while the last line includes only

$$R, \quad a_1 R, \quad b_1 R, \quad Z_1 ; \tag{82'}$$

and the final relations (70) may be reduced by (68_1) to

$$H_a Z_1 = H_b Z_1 = H_a H_b . \tag{70'}$$

29. For $n=1, 2, 3$, we prove below that every invariant of the pair of forms (54) is an integral function of the eight invariants (81), which thus form a complete system. The proof is so conducted as to show incidentally that the invariants (82) are linearly independent. The latter thus form a complete set of linearly independent invariants of the pair of forms.

Although the first seven invariants (81), together with $Z_m = Z_1^m$, completely characterize the various canonical types of two quadratic forms, they do not form a complete sytem of independent invariants. In fact, every product involving Z_m reduces, in view of (70), to $a_1^i b_1^j Z_m$ and a function of $R, \ldots$. We may restrict i and j to values $< m$. For, by multiplying (69) by $a_1^m - 1$ and by $b_1^m - 1$, we see that $a_1^m Z_m$ and $b_1^m Z_m$ equal Z_m plus a function of $R, \ldots$. Hence the present list of linearly independent invariants is now smaller than (82), lacking terms corresponding to $a_1^m Z_1$, Z_1^2, .., Z_1^{m-1}.

30. The method of obtaining simultaneous invariants from the invariants of a single form by replacing each a_i by $a_i + k b_i$ was applied in § 16 to I_a, but not to H_a. Let

$$H_{a+kb} = H_a + k^m H_b + \sum_{i=1}^{m} k^i S_i \qquad (m = 2^n - 1). \tag{83}$$

For use in § 31, we note that when $n=1$,

$$S_1 = a_2 (a_0 b_1 + a_1 b_0 + b_0 b_1) + b_2 (a_0 b_1 + a_1 b_0 + a_0 a_1). \tag{84}$$

If we interchange the a's and b's, replace k by k^{m-1}, and multiply the result by $k k^{2^n - 3} k = k^m$, we obtain the same expression as when we merely multiply a by k^m. Hence S_i and S_{m-i} are permuted by interchanging the a's and b's. Again, since $H^2 = H$,

$$S_i^2 = S_{2i}, \quad S_{2^{n-1}+i}^2 = S_{2i+1} \qquad (i < 2^{n-1}). \tag{85}$$

In view of the two results, every S_i may be obtained at once from S_1 if $n \leqq 3$

from S_1, S_3, S_5 if* $n=4$ or 5. For any n, we shall determine the values of S_1, and for $n>3$ those of S_3, and S_5 for the four cases enumerated in § 20.

$$\text{(D)}\quad H_{kb}=k^m H_b\,,\ \text{each } S_i=0.$$

$$\text{(C)}\quad H=k^m H_b+\sum_{i=0}^{n-1}(k^{m-1}b_1^{m-2}b_2)^{2^i},$$

the exponents of k and b_1 being replaced by unity if $n=1$, so that $S_1=b_1 b_2$. For $n>1$, the only non-vanishing S_i are obviously

$$S_{m-2^i}=b_1^{m-2^{i+1}}b_2^{2^i}\qquad(i=0,\ 1,\ ..,\ n-1).$$

Thus $S_1=b_1^2b_2^2$ if $n=2$, $S_1=0$ if $n>2$, $S_3=S_5=0$ if $n>3$.

$$\text{(B)}\quad H=k^m H_b+\sum_{i=0}^{n-1}\Big[\sum_{j=0}^{m-3}C_j^{m-2}k^{j+2}b_0b_2b_1^j\Big]^{2^i}\qquad(n>1).$$

If $n=1$, $S_1=b_0b_2$. The binomial coefficient C_j^{m-2} is odd if, and only if, $j=4l$ or $4l+1$. Now $x\,2^i\equiv1\equiv2^n(\text{mod } m)$ gives $x\equiv2^{n-i}$; thus $j+2=2^{n-i}$ makes C_j^{m-2} even unless $n-i=1, j=0$. Hence $S_1=(b_0b_2)^{2^{n-1}}$ for every n. To determine S_3 for $n>2$, we note that $x\,2^i\equiv3\,(\text{mod } m)$ gives $x\equiv3\,.\,2^{n-i}$. For $i>1, j+2=3\,.\,2^{n-i}$ makes C_j^{m-2} even unless $n-i=1, j=4$. For $i=1$, $j+2=2^{n-1}+1$ makes C_j even. For $i=0$, $j=1$. Hence $S_3=(b_0b_2b_1^4)^{2^{n-1}}+b_0b_2b_1$. Similarly, the four possible cases for i give

$$S_5=(b_0b_2b_1^8)^{2^{n-1}}+(b_0b_2b_1^{2^{n-1}})^2,\ n>3.$$

$$\begin{aligned}\text{(A)}\quad H&=\sum_{i=0}^{n-1}\big[(1+kf)^{m-1}\{ke+c(1+kf)\}\big]^{2^i}\\&=(1+kf)^m\textstyle\sum c^{2^i}+\sum\big[(1+kf)^{m-1}ke\big]^{2^i}\\&=\sum_{s=0}^{m}k^sf^s+\sum_{i=0}^{n-1}\Big[\sum_{j=0}^{m-1}(j+1)k^{j+1}f^je\Big]^{2^i},\end{aligned}$$

since $\sum c^{2^i}=1$, $C_s^m\equiv1$, $C_j^{m-1}\equiv j+1$ (mod 2). The terms of S_t have $j+1\equiv t\,2^{n-i}\,(\text{mod } m)$. As above, we find that†

$$S_1=f+e\,(n>1),\quad S_3=f^3+f^2e+fe^2,\quad S_5=f^5+f^4e+fe^4\,(n>2),$$

while by a special examination, $S_1=e$, if $n=1$.

---

* If $n=6$, we would need S_1, S_3, S_5, S_7, S_9, S_{11}.

† $S_7=f^7+f^6e+f^5e^2+f^3e^4$. Note that $S_3=H_b$ for $n=2$, $S_7=H_b$ for $n=3$.

We deduce the identities

$$\left.\begin{aligned}
&S_1=(a_1+b_1+a_1b_1)R\,(n=1),\quad S_1=(a_1^3-1)b_1^2R+a_1R^2+a_1^2b_1H_a\,(n=2),\\
&S_1=a_1^{2^n-3}R^{2^{n-1}}+a_1^{2^n-2}b_1H_a\ (n>2),\\
&S_3=a_1^{2^n-5}b_1^2R^{2^{n-1}}+a_1^{2^n-6}b_1R+a_1^{2^n-4}b_1^3H_a\ (n>3),\\
&S_5=a_1^{2^n-7}b_1^4R^{2^{n-1}}+a_1^{2^n-6}b_1R^2+a_1^{2^n-6}b_1^5H_a\ (n>3),
\end{aligned}\right\}\quad(86)$$

with the additional terms $(a_1^7-1)b_1^6R^2$ in S_3 if $n=3$.

DETERMINATION OF ALL THE INVARIANTS IN THE $GF[2^n]$, $n\leqq 3$.

31. Let $n=1$, so that the a_i, b_i are integers modulo 2. Then

$$I_a+H_a+a_1+1=J_a=a_2(a_0+a_1+1)+a_0a_1+a_0, \tag{87}$$

$$V_1+S_1+I_b+1=\sigma=a_2(b_0+b_1)+b_2(a_0+a_1)+a_0b_1+a_1b_0 \tag{88}$$

are invariants of the second degree defined by the earlier invariants (58), (59), (61′), (84). We may also derive σ from $J_{a+kb}=J_a+kJ_b+k\sigma$.

Any integral function of the a_i, b_i may be given the form

$$\phi=Ea_2b_2+Fa_2+Gb_2+K\quad(E,\,..,\text{ functions of }a_0,\,a_1,\,b_0,\,b_1).$$

Under the substitution (55), with $t=1$, ϕ takes the increment

$$a_2E(b_1+b_0)+b_2E(a_1+a_0)+\{E(a_1+a_0)(b_1+b_0)+F(a_1+a_0)+G(b_1+b_0)\}.$$

If ϕ is invariant the three parts must be zero (mod 2). Hence

$$E=e_1(1+b_1+b_0)+e_2b_0b_1,\quad e_i=s_i(1+a_1+a_0)+t_ia_0a_1,$$
$$F(a_1+a_0)=G(b_1+b_0),$$

where s_i and t_i are constants. Hence the invariant

$$\phi'=\phi-t_2H_aH_b-s_2J_aH_b-t_1H_aJ_b-s_1J_aJ_b$$

has $E'=0$. Then by (56), no term of ϕ' has a factor a_2b_2 or a_0b_0. This property is true of the following invariants:

$$J_a,\quad \sigma,\quad a_1b_1\sigma,\quad b_1\sigma,\quad a_1\sigma,\quad b_1(J_a+\sigma),\quad H_a,\quad b_1H_a,$$

in which the coefficient of a_2 has the respective values

$$a_0+a_1+1,\quad b_0+b_1,\quad a_1b_0b_1+a_1b_1,\quad b_0b_1+b_1,\quad a_1b_0+a_1b_1,$$
$$a_0b_1+a_1b_1+b_0b_1,\quad a_0a_1,\quad a_0a_1b_1.$$

Subtracting constant multiples of the preceding invariants from ϕ', we obtain an invariant ϕ_1 having $E_1=0$, and such that F_1 lacks the terms

$$1,\quad b_0,\quad a_1b_0b_1,\quad b_1,\quad a_1b_0,\quad a_1b_1,\quad a_0a_1,\quad a_0a_1b_1,$$

no one of which occurs in a later one of the above combinations. Then

$$F_1 = c\,a_0 + d\,a_1 + e\,a_0 b_1 + f b_0 b_1.$$

But $F_1(a_1 + a_0)$ must vanish when $b_1 = b_0$. Thus $F_1 \equiv 0$. Hence no term of ϕ_1 contains a_2 or a_0. Thus $\phi_1 = \beta_1 + a_1 \beta_2$, where the β's are functions of the b_i only. But a_1 is an invariant. Hence β_1 and β_2 must be invariants. But the above discussion shows that every invariant involving only the a_i is a linear function of J_a, H_a, a_1. Hence the β's are linear functions of J_b, H_b, b_1.

THEOREM. *Every invariant of a pair of binary quadratic forms modulo 2 is an integral function of σ and the invariants of the separate forms; every invariant is a linear function of the following twenty:*

$$H_a H_b,\ H_a J_b,\ H_b J_a,\ J_a J_b,\ a_1^i H_b,\ b_1^i H_a,\ a_1^i J_b,\ b_1^i J_a,\ a_1^i b_1^j,\ a_1^i b_1^j \sigma \quad (i, j = 0, 1). \tag{89}$$

If we eliminate $H_a = a_1 J_a$ and $H_b = b_1 J_b$, we obtain

$$a_1^i b_1^j (1,\ \sigma,\ J_a,\ J_b,\ J_a J_b) \qquad (i, j = 0, 1). \tag{89'}$$

The product of any two invariants (89′) can be reduced to a linear function of the same by use of the relations

$$\sigma J_a = a_1 \sigma + \sigma, \quad \sigma J_b = b_1 \sigma + \sigma, \tag{90}$$

and $a_1^2 = a_1$, etc. For the resultant of the forms, we have (end of § 32)

$$R = (1 + a_1 b_1)\sigma + b_1 J_a + a_1 J_b. \tag{91}$$

Then (86_1), (93), (87), (88), (64) give the other invariants in terms of (89′).

In the notations of § 28, it now follows for $n = 1$ that every invariant is an integral functions of the eight invariants (81), and that the twenty invariants given by (82′) and the first two lines of (82) form a complete set of linearly independent invariants.

32. For any n we set, in generalization of (87),

$$J_a = I_a + H_a + a_1^m - 1, \quad J_b = I_b + H_b + b_1^m - 1 \,(m = 2^n - 1). \tag{92}$$

Then, by (71) and (72),

$$H_a = a_1^m J_a,\ H_b = b_1^m J_b,\ I_a = (a_1^m - 1)(J_a - 1),\ I_b = (b_1^m - 1)(J_b - 1). \tag{93}$$

The invariants of a single form may therefore be expressed in terms of two. Hence the eight invariants (81) may be expressed in terms of six. For $n = 1$, we expressed (in § 31) all the invariants in terms of the invariants of the single forms and one additional invariant σ. But, for $n > 2$, there exists no combination C of the S_1 and invariants (81), other than R, in terms of which R can

be expressed rationally. Indeed, for the two pairs of forms under V in § 22, with $\sigma=0$ and $\sigma=1$, respectively, the invariants (81), other than R, take the same value, while $S_1=0$ by (86). When $n=1$ or 2, $S_1=\sigma$ or σ^2 for forms V. The exceptional nature of the case $n=1$ is due to the relation (86): $R=S_1+(a_1-1)(b_1-1)R$ which, by (69), enables us to express R in terms of S_1, Z_1, a_1, b_1, I_a, I_b. For $n=2$, (86) gives

$$(S_1-a_1^2 b_1 H_a)^3=(a_1^3 b_1^3+a_1^3+b_1^3)R^3,$$

so that, by (69), R^3 can be expressed in terms of S_1, Z_1, etc.

33. Next, let $n=2$. Let the general polynomial

$$\phi=\sum_{i,j}^{0,1,2,3} D_{ij}\, a_2^i b_2^j \qquad (D\text{'s functions of } a_0,\, a_1,\, b_0,\, b_1)$$

become ϕ' under transformation (55). The coefficient of t in $\phi'-\phi$ is

$$a_1\phi_{a_2}+b_1\phi_{b_2}+a_0^2(\tfrac{1}{2}\phi_{a_2^2})+b_0^2(\tfrac{1}{2}\phi_{b_2^2})+a_0 b_0\phi_{a_2 b_2}+\Sigma E_{rs}\tfrac{1}{r!\,s!}\phi_{a_2^r b_2^s}, \tag{94}$$

with $r+s\geqq 3$, the values of the E_{rs} not being required in the treatment here employed. The divisons by 2, $r!$ $s!$ are to be performed algebraically and the quotients alone interpreted in the $GF[2^2]$. A second* annihilator of an invariant ϕ is given by the coefficient of t^2 in $\phi'-\phi$; it may be obtained from (94) by applying the substitution $(a_0 a_1)(b_0 b_1)$, as follows from (55) for $n=2$. We shall designate by (k') the relation derived by applying $(a_0 a_1)(b_0 b_1)$ to a relation (k) deduced from (94).

The coefficients of $a_2^2 b_2^3$, $a_2^3 b_2^2$, $a_2 b_2^3$, $a_2^3 b_2$ in (94) give

$$a_1 D_{33}=b_1 D_{33}=a_0^2 D_{33}=b_0^2 D_{33}=0.$$

Hence

$$D_{33}=c\,(a_0^3-1)(a_1^3-1)(b_0^3-1)(b_1^3-1).$$

After subtracting $c\,I_a I_b$ from ϕ, we have $D_{33}=0$. Then, by (56), no term of ϕ has a factor $a_0^3 b_0^3$. For $D_{33}=0$, the coefficients of $a_2^2 b_2^2$, $a_2^2 b_2$, $a_2 b_2^2$, a_2^3, b_2^3, $a_2 b_2$ in (94) give

$$a_1 D_{32}=b_1 D_{23},\quad a_1 D_{31}=b_0^2 D_{23},\quad b_1 D_{13}=a_0^2 D_{32}, \tag{95}$$

$$b_1 D_{31}=b_0^2 D_{32},\quad a_1 D_{13}=a_0^2 D_{23},\quad a_0^2 D_{31}=b_0^2 D_{13}. \tag{96}$$

Let δ_{ij} be the coefficient of $b_0^i b_1^j$ in D_{32}. By $b_0\,(96_1)+b_1\,(96_1')$,

$$(b_0^3+b_1^3)D_{32}=0,\quad \delta_{10}=\delta_{20}=\delta_{01}=\delta_{02}=0,\quad \delta_{03}=\delta_{30}=\delta_{00}.$$

---

* That given by t^3 is a consequence of the other two.

By (95_3), $a_0^2 D_{32}$ is a multiple of b_1. Hence

$$a_6^2 \delta_{00} (1 + b_0^3) = 0,$$

so that δ_{00} has the factor $a_0^3 - 1$. But in ϕ, $\delta_{00} = \delta_{30}$ is multiplied by b_0^3. Since a factor $a_0^3 b_0^3$ can not occur, $\delta_{00} = 0$. Hence

$$D_{32} = \Sigma\, \delta_{ij}\, b_0^i\, b_1^j \qquad (i, j = 1, 2, 3). \tag{97}$$

By $b_0 (95_1) + b_1 (95_1')$, we have $(a_0 b_1 + a_1 b_0) D_{32} = 0$. Hence

$$a_0\, \delta_{i j-1} = a_1\, \delta_{i-1 j} \qquad (i, j = 1, 2, 3), \tag{98}$$

in which a subscript 0 is to be replaced by 3; note that in (97) each subscript take distinct values modulo 3. Since δ_{3j} is free of a_0^3, (98), for $i = 3$, requires that $a_0 \delta_{3j-1}$ and hence each δ_{3j} be a multiple of a_1. Then by (98), for $i = 1$, $a_1 \delta_{3j}$, and hence also δ_{3j}, is a multiple of a_0. Thus

$$\delta_{3j} = a_0^2 \sum_{k=1}^{3} c_{jk}\, a_1^k + a_0 \sum_{k=1}^{3} d_{jk}\, a_1^k \qquad (j = 1, 2, 3),$$

the c's and d's being constants whose subscripts may be reduced modulo 3 without causing ambiquity. Then by (98), for $i = 3$,

$$\delta_{2j} = a_0^3 \sum_{k=1}^{3} c_{j-1 k}\, a_1^{k-1} + a_0^2 \sum_{k=1}^{3} d_{j-1 k}\, a_1^{k-1} + (a_1^3 - 1) \sum_{i=0}^{3} \rho_{ji}\, a_0^i.$$

Now $a_1 \delta_{1j} = a_0 \delta_{2j-1}$, so that the latter has no terms free of a_1. Thus

$$\rho_{s1} = 0, \quad \rho_{s2} = d_{s-11}, \quad \rho_{s3} = \rho_{s0} + c_{s-11} \quad (s = 1, 2, 3),$$

$$\delta_{2j} = a_0^3 \sum_{k=2}^{4} c_{j-1k}\, a_1^{k-1} + a_0^2 \sum_{k=2}^{4} d_{j-1k}\, a_1^{k-1} + \rho_{j0} (a_0^3 - 1)(a_1^3 - 1).$$

Now the coefficients of $a_2^2 b_2^2$ in $H_b I_a$ and $H_a H_b R$ are

$$(a_0^3 - 1)(a_1^3 - 1)\, b_0^2 b_1^2, \quad a_0 a_1 b_0 b_1^2 + a_0^2 a_1^3 b_0^3 b_1^3 + a_0^3 a_1^2 b_0^2 b_1.$$

Hence by subtracting from ϕ constant multiples of

$$b_1^i H_b I_a, \qquad a_1^i b_1^j H_a H_b R \qquad (i, j = 0, 1, 2),$$

we may delete from D_{32} the terms $a_0^3 b_0^2 b_1^r$, $a_0^3 b_0^2 a_1^s b_1^r$ $(s, r = 1, 2, 3)$. Then each δ_{2r} is free of a_0^3, so that each $c_{st} = 0$, $\rho_{s0} = 0$. In the simplified form of δ_{2j}, let $k = l + 1$, then

$$\delta_{3j} = a_0 \sum_{k=1}^{3} d_{jk}\, a_1^k, \quad \delta_{2j} = a_0^2 \sum_{l=1}^{3} d_{j-1\, l+1}\, a_1^l \qquad (j = 1, 2, 3).$$

By (98), for $i = 2$, $a_1 \delta_{1j} = a_0 \delta_{2j-1}$, so that

$$\delta_{1j} = a_0^3 \sum_{l=1}^{3} d_{j-2\, l+1}\, a_1^{l-1} + (a_1^3 - 1)\, A_j' \equiv a_0^3 \sum_{l=2}^{4} d_{j-2\, l+1}\, a_1^{l-1} + (a_1^3 - 1)\, A_j,$$

where A' and A are functions of a_0. Replacing l by $l+1$ and applying (98) for $i=1$, we see that $a_0 A_{j-1}=0$, so that, by (97),

$$D_{32}=\sum_{j=1}^{3} b_1^j \{b_0^3 a_0 \sum_{l=1}^{3} d_{jl} a_1^l + b_0^2 a_0^2 \sum_{l=1}^{3} d_{j-1\, l+1} a_1^l + b_0 a_0^3 \sum_{l=1}^{3} d_{j-2\, l+2} a_1^l + b_0 \sigma_j A\},$$

where $A=(a_0^3-1)(a_1^3-1)$, and the σ_j are constants. Then by (95_3),

$$D_{13}=\sum_{j=1}^{3} b_1^{j+2}\{b_0^3 a_0^3 \Sigma + b_0^2 a_0 \Sigma + b_0 a_0^2 \Sigma\} + (b_1^3-1)\, G,$$

the sums being the same as in D_{32}. By $a_0^2(95_3') + a_1^2(95_3)$,

$$(a_0^2 b_0 + a_1^2 b_1)\, D_{13}=0.$$

Hence $a_0^2 b_0\, G=0$, so that

$$G=(b_0^3-1)\sum_{k=0}^{2} k_i a_0^i + c_3(a_0^3-1),$$

where the k_i are functions of a_1; c_3 a function of a_1, b_0. By (96_3), $b_0^2 D_{13}$ is a multiple of a_0. Hence $b_0 c_3=0$, $c_3=k_3(b_0^3-1)$. The total coefficient of $a_0^3 b_0^3$ in D_{13} must vanish; by the terms free of b_1, $k_3=0$; by the terms in b_1, each $d_{jl}=0$. By $(96_2')$, $a_0 D_{13}$ and hence each k_i is a multiple of a_1. By (96_2), $a_1 D_{13}$ and hence $a_1 G$ is a multiple of a_0, whence $a_1 k_0=0$, $k_0=0$. By subtracting from ϕ constant multiples of $a_1^i H_a I_b$ $(i=0, 1, 2)$, we may delete from D_{13} the terms

$$a_0 a_1^r (b_0^3-1)(b_1^3-1) \qquad (r=1, 2, 3).$$

Then $k_1=0$ in G, so that

$$D_{32}=b_0 A \sum_{j=1}^{3} b_1^j \sigma_j, \quad D_{13}=(b_0^3-1)(b_1^3-1)\, k_2 a_0^2, \quad k_2=\sum_{j=1}^{3} g_j a_1^j.$$

By (95_1) and $(95_1')$, $D_{23}=(b_0^3-1)(b_1^3-1)\, F$, where F is a function of a_0 and a_1, free of a_0^3. By $(96_2')$, $a_0^3 k_2=a_1^2 F$. Hence $k_2=0$, $D_{13}=0$. By (96_2), $a_0 F=0$, $F=0$, $D_{23}=0$. By (95_2), $(95_2')$, $D_{31}=AK$, where, as above, $A=(a_0^3-1)(a_1^3-1)$, and K is free of b_0^3. By $(96_1')$, $b_0 K=b_0 \Sigma\, b_1^{j+2}\sigma_j$, so that $K=\Sigma\, b_1^{j+2}\sigma_j$. Then (96_1) gives

$$\Sigma\, b_1^j \sigma_j = b_0^3 \Sigma\, b_1^j \sigma_j, \qquad \sigma_j=0\ (j=1, 2, 3).$$

We have now proved (99) and hence by (56) also (100):

$$D_{33}=D_{32}=D_{23}=D_{31}=D_{13}=0. \tag{99}$$

No term of ϕ *has a factor* $a_0^3 b_0^3$, $a_0^3 b_0^2$, $a_0^2 b_0^3$, $a_0^3 b_0$, $a_0 b_0^3$. (100)

In (94) the coefficients of a_2^3, b_2^3, a_2, b_2 now give

$$a_1 D_{30} + b_1 D_{21} = b_0^2 D_{22}, \qquad b_1 D_{03} + a_1 D_{12} = a_0^2 D_{22}, \tag{101}$$
$$a_0^2 D_{30} + b_0^2 D_{12} = b_1 D_{11}, \qquad b_0^2 D_{03} + a_0^2 D_{21} = a_1 D_{11}. \tag{102}$$

The relations derived by applying $(a_0 a_1)(b_0 b_1)$ are designated (101′), (102′).

Applying the result (100) to (101_1), we see that D_{22} does not contain a_0^3, $a_0^2 b_0$, $a_0 b_0$; nor $a_0 b_0^2$, b_0^3 by (101_2). Applying (102′) similarly, we get

$$D_{22} = a_0^2 b_0^2 d_1 + a_0^2 d_2 + a_0 d_3 + b_0^2 d_4 + b_0 d_5 + d_6 ,$$
$$D_{11} = a_0 b_0 d_7 + a_0^2 d_8 + a_0 d_9 + b_0^2 d_{10} + b_0 d_{11} + d_{12},$$

in which the d_i (and the e_i below) are functions of a_1, b_1.

By (102), D_{30} must be free of $a_0 b_0$ and a_0, since neither $a_0^3 b_0$ nor a_0^3 occur in $b_0^2 D_{12}$ or $b_1 D_{11}$. In this manner (102) and (101′) show that D_{30} is free of $a_0 b_0$, a_0, $a_0^2 b_0^2$, a_0^2; D_{03} free of $a_0 b_0$, b_0, $a_0^2 b_0^2$, b_0^2; D_{12} free of $a_0 b_0$, b_0, $a_0^2 b_0^2$, a_0^2; D_{21} free of $a_0 b_0$, a_0, $a_0^2 b_0^2$, b_0^2.

We shall simplify ϕ by subtracting constant multiples of certain invariants satisfying (99). By (57) and (61), the coefficients of $a_2^3 b_0^3$ in R^3 and Z_1 are obviously $1 + a_1^3 b_1^3$, $a_1^2 b_1$. Multiplying the former by 1, a_1^k, b_1^k $(k = 1, 2, 3)$, and the latter by $a_1^i b_1^j$ $(i, j = 0, 1, 2)$, we obtain 16 linearly independent combinations of $a_1^r a_1^s$ $(r, s = 0, 1, 2, 3)$. Hence we may assume that D_{30} is free* of b_0^3. Employing $b_1^r I_a$, we may assume that the coefficient of $a_0^3 a_0$ is a multiple of a_1. In $H_a R$, the coefficient of a_2^3 is $a_0^3 a_1^2 b_1^2 + a_0^2 a_1^3 b_0 b_1 + a_0 a_1 b_0^2$; that in $H_a R^2$, the square of the latter; that in $(a_1^3 - 1) Z_1$ is $a_0^2 b_0 (a_1^3 - 1)(b_1^3 - 1)$. Employing $a_1^i H_a R^2$, $a_1^i b_1^j H_a R$, $(a_1^3 - 1) Z_1$ $(i, j = 0, 1, 2)$, we may assume that the coefficient of $a_0^2 b_0$ in D_{30} is $\sum_{i=1}^{3} c_i b_1^i$. The coefficients of a_2^3 in $a_1^i (b_1^3 - 1) H_a R$ and $Z_1^2 + a_1^2 b_1 Z_1$ are

$$a_0 b_0^2 a_1^{i+1} (b_1^3 - 1), \qquad a_0 b_0^2 (a_1^3 - 1)(b_1^3 - 1).$$

Hence we may take the coefficient of $a_0 b_0^2 b_1^3$ to be zero.

We next subtract invariants satisfying (99) and lacking a_2^3. Employing $a_1^r I_b$ $(r = 0, 1, 2, 3)$, $a_1^i b_1^j H_b R$ $(i, j = 0, 1, 2)$, we may reduce the coefficient of b_0^3 in D_{03} to $\sum_{i=1}^{3} k_i b_1^i$. The coefficients of $(a_1^3 - 1) H_b R$ and $H_b R^2 + a_1^2 b_1^2 H_b R$ are $a_0^2 b_0 b_1 (a_1^3 - 1)$, $a_0 b_0^2 b_1^2 (a_1^3 - 1)$. Multiplying these by $b_1^i (i = 0, 1, 2)$, we may assume that in D_{03} the coefficients of $a_0^2 b_0 a_1^3$ and $a_0 b_0^2 a_1^3$ are constants.

---

* The invariants used later lack $a_2^3 b_0^3$. At each stage the invariants used lack all terms previously deleted in ϕ.

Without introducing a_2^3 or b_2^3, we subtract constant multiples of $a_1^i b_1^j H_a H_b$ $(i, j = 0, 1, 2)$ and eliminate the terms $a_1^r b_1^s$ $(r, s = 1, 2, 3)$ multiplying $a_0^2 b_0^2$ in D_{22}. Hence

$$D_{30} = a_0^3 e_1 + a_0^2 b_0 \sum_{i=1}^{3} c_i b_1^i + a_0 b_0^2 e_2 + b_0^2 e_3 + b_0 e_4 + e_5,$$
$$D_{03} = a_0^3 e_6 + b_0^3 \sum_{i=1}^{3} k_i b_1^i + a_0^2 b_0 e_7 + a_0 b_0^2 e_8 + a_0^2 e_9 + a_0 e_{10} + e_{11},$$

where e_1 is a multiple of a_1, e_2 lacks b_1^3, while the coefficients of a_1^3 in e_7 and e_8 are constants, and $d_1 = \sum_{i=0}^{3} r_i a_1^i + \sum_{i=1}^{3} s_i b_1^i$. From (101′),

$$D_{12} = a_0^2 b_0 e_6 + a_0 b_0^2 (e_7 + a_1^2 d_1) + a_0 b_0 e_9 + a_0 a_1^2 d_2 + b_0^3 e_8 + b_0 e_{10} + a_1^2 d_3 + (a_0^3 - 1) e_{12},$$
$$D_{21} = a_0^3 \sum_{i=1}^{3} c_i b_1^i + a_0^2 b_0 (e_2 + b_1^2 d_1) + a_0 b_0 e_3 + a_0 e_4 + b_0 b_1^2 d_4 + b_1^2 d_5 + (b_0^3 - 1) e_{13},$$
$$a_1 d_4 = a_1 d_6 = b_1 d_2 = b_1 d_6 = 0, \quad e_1 + e_5 = b_1^2 d_3, \quad e_{11} + a_1^2 d_5 = \sum_{i=1}^{3} k_i b_1^i.$$

As shown above, D_{12} is free of $a_0 b_0$, b_0; D_{21} free of $a_0 b_0$, a_0. Hence e_3, e_4, e_9, e_{10} are zero. In relation (101_1) the coefficients of a_0^3 and $a_0^2 b_0$ give

$$a_1 e_1 = \sum_{i=1}^{3} c_i b_1^{i+1}, \quad b_1 e_2 = (b_1^3 + 1) d_1 + a_1 \Sigma c_i b_1^i.$$

By the first, each $c_i = 0$, $a_1 e_1 = 0$, $e_1 = 0$, since e_1 is a multiple of a_1. By the second and the above properties of e_2, d_1, we get $e_2 = 0$, $d_1 = 0$. The coefficients of b_0^3 and $a_0 b_0^2$ in (101_2) now give

$$a_1 e_8 = \sum_{i=1}^{3} k_i b_1^{i+1}, \quad a_1 e_7 = b_1 e_8.$$

In e_7 and e_8 the coefficients of a_1^3 are constants. Hence $k_i = 0$, $e_8 = 0$, $e_7 = c(a_1^3 - 1)$, c a constant. By the coefficient of $a_0^2 b_0^2$ in (102_1), $e_6 = 0$. The further conditions from (101) are now

$$d_2 = d_3 = d_4 = d_6 = 0, \quad d_5 = b_1 e_{13} = b_1 e_7, \quad a_1 e_5 = a_1 e_{12} = b_1 e_{11} = 0.$$

The earlier conditions now give $e_5 = 0$, $e_{11} = b_1 a_1^2 e_7 = 0$. Hence

$$D_{22} = b_0 b_1 e_7, \quad D_{30} = 0, \quad D_{03} = a_0^2 b_0 e_7, \quad D_{12} = a_0 b_0^2 e_7 + (a_0^3 - 1) e_{12},$$
$$D_{21} = (b_0^3 - 1) e_{13} + b_1^3 e_7, \quad e_7 = c(a_1^3 - 1), \quad b_1 e_{13} = b_1 e_7, \quad a_1 e_{12} = 0.$$

Then (102_1) gives $e_{12} = 0$, e_7 a multiple of b_1, whence $e_7 = 0$. Then (102_2) gives $e_{13} = 0$. Hence $b_0 D_{11} = a_0 D_{11} = 0$ by (102′). But no term has a factor $a_0^3 b_0^3$. Hence

$$D_{22} = D_{11} = D_{30} = D_{03} = D_{12} = D_{21} = 0, \tag{103}$$

No term of ϕ *has a factor* $a_0^2 b_0^2$, $a_0 b_0$, a_0^3, b_0^3, $a_0 b_0^2$, $a_0^2 b_0$. (104)

In view of (99), (100), (103), (104), we have

$$\phi = D_{00} + a_2 D_{10} + a_2^2 D_{20} + b_2 D_{01} + b_2^2 D_{02}, \tag{105}$$

where each D_{ij} is a linear function of a_0, a_0^2, b_0, b_0^2, with coefficients involving a_1, b_1. Subtracting $a_1^r b_1^s R$ $(r, s \overline{\gtrless} 3)$ from ϕ, we may assume that D_{20} is free of b_0^2. In $a_1^i b_1^r H_a$, $b_1^{i+1}(R^2 + a_1^2 b_1^2 R)$, for $i = 0, 1, 2$; $r = 0, .., 3$, the coefficients of $a_2^2 a_0^2$ are $a_1^k b_1^r$ $(k = 1, 2, 3)$, b_1^{i+2}; hence in D_{20} the coefficient of a_0^2 may be made a constant l. Thus

$$D_{20} = l a_0^2 + C_1 a_0 + C_2 b_0 + C_3 \quad (C\text{'s functions of } a_1, b_1).$$

Next, H_b and $a_1^2 R^2 + a_1 b_1^2 R + b_1 H_a$ are free of a_2^2 and have $b_0^2 b_1^2$ and $b_0^2 a_1^3$ as the coefficients of b_2^2. Multiplying the former by $b_1^i a_1^r$ and the latter by a_1^i $(i \overline{\gtrless} 2,\ r \leqq 3)$, we may assume that the coefficient of b_0^2 in D_{02} is a constant λ. Thus

$$D_{02} = \lambda b_0^2 + C_4 a_0^2 + C_5 a_0 + C_6 b_0 + C_7 \quad (\lambda \text{ constant}),$$

$$D_{10} = a_0^2 C_8 + a_0 C_9 + b_0^2 C_{10} + b_0 C_{11} + C_{12}, \quad D_{01} = a_0^2 C_{13} + a_0 C_{14} + b_0^2 C_{15} + b_0 C_{16} + C_{17}.$$

For ϕ given by (105), the terms free of a_2, b_2 in (94) give

$$a_1 D_{10} + b_1 D_{01} + a_0^2 D_{20} + b_0^2 D_{02} = 0. \tag{106}$$

From this and the relation derived by $(a_0 a_1)(b_0 b_1)$, we get

$$C_i = 0\ (i = 1, .., 8, 10, 12, 13, 15, 17), \quad C_9 = l a_1^2, \quad C_{11} = C_{14}, \quad C_{16} = \lambda b_1^2,$$
$$a_1 C_9 + b_1 C_{14} = l, \quad a_1 C_{11} + b_1 C_{16} = \lambda.$$

By the last two, $l = \lambda = 0$. Then $b_1 C_{11} = a_1 C_{11} = 0$,

$$C_{11} = C_{14} = c\pi, \quad \pi = (a_1^3 - 1)(b_1^3 - 1).$$

From ϕ we subtract c times the invariant

$$\pi R^2 = \pi(a_2 b_0 + b_2 a_0) = (a_1^3 + b_1^3 + 1) R^2 + a_1^2 b_1^2 R + a_1 b_1 (H_a + H_b),$$

and have every $C_i = 0$. Then $\phi = D_{00}$ is free of a_2, b_2 and hence of a_0, b_0 by (56), so that ϕ is reduced to zero by subtracting multiples of $a_1^r b_1^s$ $(r, s \leqq 3)$.

The invariants which we have subtracted from ϕ are seen by inspection to be linearly equivalent to the invariants (82).

THEOREM.* *Every invariant of a pair of quadratic forms in the* $GF[2^2]$

* In an earlier proof, I first determined the linearly independent invariants of weight $\equiv 1 \pmod 3$; then those of weight $\equiv 2$ by squaring the preceding; finally, those of weight $\equiv 0$ by noting that if J denotes the aggregate of the terms free of a_1 and b_1 in ϕ, then $\phi = \pi J + K$, where $K = (a_1^3 b_1^3 + a_1^3 + b_1^3) I$ is found by multiplying the invariants of weight 1 by a_1^2 and b_1^2, in turn. Those of type πJ contain only D_{33}, D_{30}, D_{03}, D_{21}, D_{12}, D_{00} and are found very easily.

is an integral function of the 8 *independent invariants* (81)*; indeed, a linear combination of the* 144 *linearly independent invariants* (82), *for* $n=2$.

34. For the $GF[2^n]$, the general polynomial

$$\phi = \Sigma\, D_{rs}\, a_2^r\, b_2^s \quad (r,\ s = 0, 1, \ldots, m = 2^n - 1) \tag{107}$$

receives under the transformation (55) an increment in which the coefficient of $a_2^\rho b_2^\sigma$ is

$$\sum_{\substack{i=0,\ldots,m-\rho\\ j=0,\ldots,m-\sigma}}' P_{ij}\, C_i^{\rho+i}\, C_j^{\sigma+j}\, D_{\rho+i\,\sigma+j}, \quad P_{ij} \equiv (t a_1 + t^2 a_0)^i (t b_1 + t^2 b_0)^j, \tag{108}$$

the C's being binomial coefficients and the accent denotes that i and j are not both zero. Let $T_{k\rho\sigma}$ denote the coefficient of t^k in (108), π_{kij} that of t^k in P_{ij}, after the exponents have been reduced by means of $t^{m+1} = t$. Such a reduction occurs only for $i + j \geqq 2^{n-1}$. For $n > 1$, we have*

$$T_{1\rho\sigma} = (\rho+1)\, a_1 D_{\rho+1\,\sigma} + (\sigma+1)\, b_1 D_{\rho\,\sigma+1} + \Sigma\, \pi_{1ij}\, C_i^{\rho+i}\, C_j^{\sigma+j}\, D_{\rho+i\,\sigma+j}$$
$$(i = 0, \ldots, m-\rho;\ j = 0, \ldots, m-\sigma;\ i+j \geqq 2^{n-1}), \tag{109}$$

the final sum being absent if $\rho + \sigma > 2m - 2^{n-1}$;

$$T_{2\rho\sigma} = (\rho+1)\, a_0 D_{\rho+1\,\sigma} + (\sigma+1)\, b_0 D_{\rho\,\sigma+1} + a_1^2\, C_2^{\rho+2} D_{\rho+2\,\sigma} + b_1^2\, C_2^{\sigma+2}\, D_{\rho\,\sigma+2}$$
$$+ a_1 b_1 (\rho+1)(\sigma+1)\, D_{\rho+1\,\sigma+1} + \Sigma\, \pi_{2ij}\, C_i^{\rho+i}\, C_j^{\sigma+j}\, D_{\rho+i\,\sigma+j}$$
$$(i \leqq m-\rho,\ j \leqq m-\sigma,\ i+j \geqq 1 + 2^{n-1}), \tag{110}$$

the final sum being absent if $\rho + \sigma > 2m - 2^{n-1} - 1$.

In this modular theory, it appears to be sufficient to require the vanishing of the coefficients $T_{k\rho\sigma}$ of t^k for $k = 1, 2, 2^2, \ldots, 2^{n-1}$ (cf. *Transactions*, l. c., pp. 210, 213, 214, etc.). For $n > 2$,

$$\begin{aligned} T_{4\rho\sigma} = {} & a_0^2\, C_2^{\rho+2}\, D_{\rho+2\sigma} + b_0^2\, C_2^{\sigma+2}\, D_{\rho\sigma+2} + a_0 b_0 (\rho+1)(\sigma+1)\, D_{\rho+1\,\sigma+1} \\ & + a_0 a_1^2\, C_3^{\rho+3} D_{\rho+3\sigma} + a_1^2 b_0\, C_2^{\rho+2}(\sigma+1)\, D_{\rho+2\,\sigma+1} + a_0 b_1^2\, C_2^{\sigma+2}(\rho+1)\, D_{\rho+1\,\sigma+2} \\ & + b_0 b_1^2\, C_3^{\sigma+3}\, D_{\rho\,\sigma+3} + a_1^4\, C_4^{\rho+4}\, D_{\rho+4\sigma} + a_1^3 b_1\, C_3^{\rho+2}(\sigma+1)\, D_{\rho+3\,\sigma+1} \\ & + a_1^2 b_1^2\, C_2^{\rho+2}\, C_2^{\sigma+2}\, D_{\rho+2\,\sigma+2} + a_1 b_1^3\, C_3^{\sigma+3}(\rho+1)\, D_{\rho+1\,\sigma+3} + b_1^4\, C_4^{\sigma+4}\, D_{\rho\sigma+4} \\ & + \Sigma\, \pi_{4\rho\sigma}\, C_i^{\rho+i}\, C_j^{\sigma+j}\, D_{\rho+i\,\sigma+j}\ (i \leqq m-\rho,\ j \leqq m-\sigma,\ i+j \geqq 2 + 2^{n-1}). \end{aligned} \tag{111}$$

If we write ρ and i to the scale of base 2, $C_i^{\rho+i}$ is odd if each coordinate of i is less than or equal to the corresponding coordinate of ρ, viz., if the partition of $\rho + i$ into ρ and i takes place in the coefficients of the various powers of 2

* Here and below, terms preceding the summation signs are to be suppressed if they contain a D with subscript $> m$.

separately. In the contrary case, $C_i^{\rho+i}$ is a multiple of the modulus 2. For example, since $m=2^n-1$, we have when $n>1$,

$$C_2^{m+1}\equiv 0,\quad C_2^{m+2}\equiv 0,\quad C_2^{m+3}\equiv 1 \pmod 2.$$

Hence we have, by inspection,

$$T_{1mm-1}\equiv b_1 D_{mm},\ T_{1m-1m}\equiv a_1 D_{mm},\ T_{2mm-1}\equiv b_0 D_{mm},\ T_{2m-1m}\equiv a_0 D_{mm}.$$

For an invariant ϕ, these must vanish. Thus

$$D_{mm}=d\,(a_0^m-1)\,(b_0^m-1)\,(a_1^m-1)\,(b_1^m-1).$$

Hence $\phi-d\,I_a I_b$ has $D_{mm}=0$. For $n\geqq 3$, various D's are now necessarily zero, so that the above T's simplify materially. In fact, the special relations discussed at any stage may be chosen so that the coefficients of the D's involve a_i and b_i only in the combinations $a_0^{2^i}$, $b_0^{2^i}$, $a_1^{2^i}$, $b_1^{2^i}$. Thus the effective parts* of the conditions (108), when used in a convenient sequence, are given by $i=0$ or $j=0$ and so may be determined by inspection.

35. Let next $n=3$. As in § 34, we may set $D_{77}=0$. By (56) no term of ϕ has the factor $a_0^7 b_0^7$. Thus $a_0 D=b_0 D=0$ imply $D=0$. In T_{171}, $i=0$, $j=4, 5, 6$; but $j=6$ leads to D_{77}, $j=5$ gives $C_5^{1+5}\equiv 0$, while $j=4$ gives $b_0^4 D_{75}=0$. Similarly, T_{135} gives $a_0^4 D_{75}=0$. Permuting the a's and b's, $T_{117}=a_0^4 D_{57}$, $T_{153}=b_0^4 D_{57}$. Hence $D_{75}=D_{57}=0$. For $D_{77}=0$,

$$T_{272}=b_0 D_{73},\quad T_{263}=a_0 D_{73},\quad T_{227}=a_0 D_{37},\quad T_{236}=b_0 D_{37},$$

whence $D_{73}=D_{37}=0$. In view of the latter,

$$T_{172}=b_0^4 D_{76},\quad T_{163}=b_0^4 D_{67},\quad T_{127}=a_0^4 D_{67},\quad T_{136}=a_0^4 D_{76},$$

whence $D_{76}=D_{67}=0$. Next,

$$T_{151}=b_0^4 D_{55},\quad T_{232}=b_0 D_{33},\quad T_{464}=b_0^2 D_{66};$$

thus $T_{115}=a_0^4 D_{55}$, etc., so that the three D's vanish. Hence

$$D_{77}=D_{76}=D_{75}=D_{73}=D_{67}=D_{66}=D_{57}=D_{55}=D_{37}=D_{33}=0. \tag{112}$$

The remaining 54 D's have non-vanishing values in R^7 or $H_a R^7$. By (56),

No term of ϕ contains $a_0^7 b_0^i$, $a_0^i b_0^7$ $(i=7, 6, 5, 3)$, $a_0^6 b_0^6$, $a_0^5 b_0^5$, $a_0^3 b_0^3$. (113)

---

* In the final sums in (109), .., certain of the π's vanish for $n>2$. For example, if $n=3$, $\pi_{1ij}=0$ for ij or $ji=50, 41, 54, 64$; $\pi_{2ij}=0$ for $i+j=6$ $(i\neq 3)$; $\pi_{4ij}=0$ for $ij=60, 42, 24, 06, 62, 44, 26$. But at the stage at which the relation is used the coefficient of such a factor π is zero, so that there is no gain in employing that fact that certain of the π vanish.

After deleting the D's in (112), $T_{\kappa\rho\sigma}$ for $\kappa = 1, 2, 4$, $\rho, \sigma = 70, 61, 52, 43, 64, 62, 54, 51, 32, 31$ give binomial relations* involving only the following twelve D_{ij}:

$$D_{74},\ D_{72},\ D_{71},\ D_{65},\ D_{63},\ D_{56},\ D_{53},\ D_{47},\ D_{36},\ D_{35},\ D_{27},\ D_{17}. \tag{114}$$

$$b_1 D_{71} = b_0^4 D_{74},\quad a_1 D_{71} = b_0^4 D_{65},\quad b_1 D_{53} = b_0^4 D_{56},\quad a_1 D_{53} = b_0^4 D_{47}, \tag{115}$$

$$a_1 D_{74} = b_1 D_{65},\quad a_1 D_{72} = b_1 D_{63},\quad a_0^4 D_{72} = b_0^4 D_{36},\quad a_0^4 D_{71} = b_0^4 D_{35}; \tag{116}$$

$$b_0 D_{71} = b_1^2 D_{72},\quad a_0 D_{71} = b_1^2 D_{63},\quad b_0 D_{53} = a_1^2 D_{72},\quad a_0 D_{53} = a_1^2 D_{63}, \tag{117}$$

$$a_0 D_{74} = b_0 D_{65},\quad a_0 D_{72} = b_0 D_{63},\quad a_1^2 D_{74} = b_1^2 D_{56},\quad a_1^2 D_{71} = b_1^2 D_{53}; \tag{118}$$

$$b_0^2 D_{72} = b_1^4 D_{74},\quad b_0^2 D_{63} = b_1^4 D_{65},\quad a_0^2 D_{72} = b_1^4 D_{56},\quad a_0^2 D_{63} = b_1^4 D_{47}, \tag{119}$$

$$a_0^2 D_{74} = b_0^2 D_{56},\quad a_0^2 D_{71} = b_0^2 D_{53},\quad a_1^4 D_{72} = b_1^4 D_{36},\quad a_1^4 D_{71} = b_1^4 D_{35}. \tag{120}$$

The binomial relations $T_{\kappa\sigma\rho}$, with the same ρ, σ, may be derived by interchanging the a's and b's (and hence permuting the subscripts of D_{ij}); they will be designated (115′).

By $b_0 (116_1) + b_1 (118_1)$ and $b_0^3 (115_1) + b_0^2 b_1 (117_1) + b_1^3 (119_1)$,

$$(a_1 b_0 + a_0 b_1) D_{74} = 0, \qquad (b_0^7 + b_1^7) D_{74} = 0.$$

The discussion of these is similar to that in § 33. By the second and $(115_4')$,

$$D_{74} = \Sigma \delta_{ij} b_0^i b_1^j \qquad (i, j = 1, \ldots, 7). \tag{121}$$

Then the first gives (98) for $i, j \leqq 7$. But, by (113), δ_{7j} is free of a_0^7, a_0^6, a_0^5, a_0^3. Then (98), for $i = 7$, $i = 1$, shows that δ_{7j} is a multiple of $a_1 a_0$:

$$\delta_{7j} = a_0^4 \sum_{k=1}^{7} c_{jk} a_1^k + a_0^2 \sum_{k=1}^{7} d_{jk} a_1^k + a_0 \sum_{k=1}^{7} e_{jk} a_1^k \qquad (j = 1, \ldots, 7),$$

the c, d, e being constants whose subscripts may be reduced modulo 7. Then (98), for $i = 7$, gives

$$\delta_{6j} = a_0^5 C_j + a_0^3 D_j + a_0^2 E_j + (a_1^7 - 1) \Gamma_j, \qquad C_j = \sum_{k=1}^{7} c_{j-1k} a_1^{k-1}, \ldots .$$

We may introduce a term from Γ_j into C_j and set

$$C_j = \sum_{k=2}^{8} c_{j-1k} a_1^{k-1} = \sum_{l=1}^{7} c_{j-1\,l+1} a_1^l \qquad (k = l + 1).$$

A similar modification may be made in D_j, E_j. By (98), for $i = 6$, $a_0 \delta_{6j-1}$ and hence $a_0 \Gamma_{j-1}$ is a multiple of a_1; thus $a_0 \Gamma_{j-1} = 0$. By (113), δ_{6j} lacks a_0^7. Hence $\Gamma_{j-1} = 0$ for every j, so that

$$\delta_{6j} = a_0^5 \sum_{l=1}^{7} c_{j-1\,l+1} a_1^l + a_0^3 \sum_{l=1}^{7} d_{j-1\,l+1} a_1^l + a_0^2 \sum_{l=1}^{7} e_{j-1\,l+1} a_1^l .$$

---

*Of these T_{464}, T_{462}, T_{154}, T_{151}, T_{232}, T_{231} give identities.

By (98), for $i=6$, $\delta_{5j}=a_0^6\,C'_j+a_0^4\,D'_j+a_0^3\,E'_j+(a_1^7-1)\,\Gamma'_j$, where we may set

$$C'_j=\sum_{\lambda=1}^{7} c_{j-2\ \lambda+1}\,a_1^{\lambda-1}+c_{j-22}\,(a_1^7-1)=\sum_{\lambda=2}^{8} c_{j-2\ \lambda+1}\,a_1^{\lambda-1}=\sum_{l=1}^{7} c_{j-2\ l+2}\,a_1^{l},$$

and similarly for D'_j, E'_j. By (98), for $i=5$, $a_0\,\delta_{5j-1}$ and hence $a_0\,\Gamma'_{j-1}$ is a multiple of a_1. But Γ' lacks a_0^7 by (113). Hence $\Gamma'=0$,

$$\delta_{5j}=a_0^6\sum_{l=1}^{7} c_{j-2\ l+2}\,a_1^l+a_0^4\sum_{l=1}^{7} d_{j-2\ l+2}\,a_1^l+a_0^3\sum_{l=1}^{7} e_{j-2\ l+2}\,a_1^l,$$

$$\delta_{4j}=a_0^7\sum_{l=1}^{7} c_{j-3\ l+3}\,a_1^l+a_0^5\sum_{l=1}^{7} d_{j-3\ l+3}\,a_1^l+a_0^4\sum_{l=1}^{7} e_{j-3\ l+3}\,a_1^l+(a_1^7-1)\,\varepsilon_j.$$

By (98), for $i=4$, $a_0\,\delta_{4j-1}$ and hence $a_0\,\varepsilon_{j-1}$ is a multiple of a_1. Thus

$$\varepsilon_j=e_j\,(a_0^7-1),\ e_j \text{ a constant.}$$

Now the coefficients of $a_0^7a_2^7b_2^4$ in $H_b\,I_a$ and $H_a\,H_b\,R^3$, which satisfy (112), are

$$(a_1^7-1)\,b_0^4\,b_1^6,\qquad a_1^6\,b_0^4\,b_1^5.$$

Multiplying the former by b_1^i and the latter by $a_1^i\,b_1^j$ $(i,j=0,\,..,\,6)$, and subtracting constant multiples of the products from ϕ, we may delete the terms

$$a_0^7\,b_0^4\,b_1^r,\qquad a_0^7\,b_0^4\,a_1^r\,b_1^s\qquad\qquad (r,s=1,\,..,\,7),$$

from D_{74}. Then δ_{4r} lacks a_0^7. Hence the total coefficient of a_0^7 in the above expression for δ_{4j} must vanish. Thus

$$c_{jk}=0,\qquad \varepsilon_j=0\qquad\qquad (j,k=1,\,..,\,7).$$

Since δ_{3j} lacks a_0^7, by (113), the earlier argument gives

$$\delta_{3j}=a_0^6\sum_{l=1}^{7} d_{j-4\,l+4}\,a_1^l+a_0^5\sum_{l=1}^{7} e_{j-4\,l+4}\,a_1^l,$$

$$\delta_{2j}=a_0^7\sum_{l=1}^{7} d_{j-5\,l+5}\,a_1^l+a_0^6\sum_{l=1}^{7} e_{j-5\,l+5}\,a_1^l+s_j\,A,$$

$$\delta_{1j}=a_0\sum_{l=1}^{7} d_{j-6\,l+6}\,a_1^l+a_0^7\sum_{l=1}^{7} e_{j-6\,l+6}\,a_1^l+t_j\,A,$$

where $A=(a_0^7-1)\,(a_1^7-1)$, s and t constants. Since the subscripts of d and e are taken modulo 7, (121) may not be written in the form

$$D_{74}=\sum_{i,j}^{1,..,7}\left\{b_0^i b_1^j\left(a_0^{9-i}\sum_{l=1}^{7} d_{j+i\ l-i}\,a_1^l+a_0^{8-i}\sum_{l=1}^{7} e_{j+i\ l-i}\,a_1^l\right)+b_1^j\,B_j\,A\right\},$$

where $B_j = b_0^2 s_j + b_0 t_j$. Then $(115_4')$ gives

$$D_{35} = \sum_{i,j}^{1,..,7} b_0^i b_1^{j-1} \left(a_0^{13-i} \sum_{l=1}^{7} d_{j+i\ l-i} a_1^l + a_0^{12-i} \sum_{l=1}^{7} e_{j+i\ l-i} a_1^l\right) + (b_1^7 - 1)\, G,$$

where G is a function of a_0, a_1, b_0. Now

$$a_1^4 b_1^2 (115_3') + a_0^4 b_0^2 (117_3') + a_0^4 b_1^2 (119_3') : (a_0^5 b_0^2 + a_1^5 b_1^2) D_{35} = 0.$$

After a simple change of summation indices, this reduces to

$$a_0^5 b_0^2\, G = 0.$$

For $G = \Sigma c_i a_0^i$, the latter gives $b_0 c_i = 0$ $(i = 1, .., 6)$, $b_0 (c_0 + c_7) = 0$,

$$G = (b_0^7 - 1) \sum_{i=0}^{6} k_i a_0^i + c_7 (a_0^7 - 1),$$

where the k_i are functions of a_1; c_7 a function of a_1, b_0, free of b_0^7. By $(120_2')$, $a_0^2 D_{35}$ is a multiple of b_0. Hence $a_0^2 \sum_{i=0}^{6} k_i a_0^i = 0$, $k_i = 0$. By (116_4), $b_0^4 D_{35}$ and hence $b_0^4 c_7$ is a multiple of a_0. Thus $c_7 = 0$, $G = 0$. By (113), D_{35} lacks $a_0^7 b_0^6$, $a_0^6 b_0^6$. Hence every d and e vanish. Thus

$$D_{35} = 0, \quad D_{74} = \beta A, \quad \beta = \sum_{j=1}^{7} b_1^j (b_0^2 s_j + b_0 t_j), \quad A = (a_0^7 - 1)(a_1^7 - 1).$$

By $(115_3')$, (118_1), $a_0 D_{65} = b_0 D_{65} = 0$, whence $D_{65} = 0$ by (113). By $(118_4')$, $b_1 D_{17} = 0$. Then by $(115_2')$, (120_1), $a_0 D_{56} = b_0 D_{56} = 0$, $D_{56} = 0$. Thus $(119_2')$, $(119_4')$, $D_{36} = 0$. By $(116_1')$, $b_1 D_{47} = 0$. Then by (119_2) and (119_4), $D_{63} = 0$. By (116_4), $a_0 D_{71} = 0$. Then (120_2) and (117_4), $D_{53} = 0$. By (116_2), (118_2), $D_{72} = AQ$, where by (113), Q lacks b_0^7, b_0^6, b_0^5, b_0^3. Then (119_1) requires that Q be independent of b_0. By (117_1), $b_1^2 D_{72} = b_0 D_{71} = 0$. Hence $Q = c\,(b_1^7 - 1)$. As above $a_0 D_{71} = 0$, whence $D_{71} = 0$. Then $D_{74} = 0$ by (115_1), $D_{72} = 0$ by (119_1). By $(116')$, $(115_2')$, (115_4), D_{47}, D_{27}, D_{17} are multiples of $B = (b_0^7 - 1)(b_1^7 - 1)$. Then by (113) and $(115_1')$, $(117_1')$, $(119_1')$, we get $D_{47} = a_0^4 r L$, $D_{27} = a_0^2 r a_1^4 L$, $D_{17} = a_0 r a_1^6 L$, where r is a function of a_1 such that $r(a_1^7 - 1) = 0$, and hence a multiple of a_1. Hence after subtracting constant multiples of $a_1^i H_a I_b$, we have $r = 0$. Hence all the D_{ij} in (114) now vanish. Then by (56), ϕ has no

$$a_0^7 b_0^i,\ a_0^i b_0^7\ (i = 4, 2, 1),\ a_0^6 b_0^5,\ a_0^5 b_0^6,\ a_0^6 b_0^3,\ a_0^3 b_0^6,\ a_0^5 b_0^3,\ a_0^3 b_0^5. \qquad (122)$$

Since the 22 D's in (112) and (114) vanish, T_{kll} $(k, l = 1, 2, 4)$ give

$$a_0^4 D_{51} = b_0^4 D_{15}, \quad a_1 D_{54} = b_1 D_{45}, \quad a_1 D_{32} + b_1 D_{23} = a_0^4 D_{62} + b_0^4 D_{26}, \qquad (123)$$

$$a_0 D_{32} = b_0 D_{23}, \quad a_1^2 D_{31} = b_1^2 D_{13}, \quad a_1^2 D_{64} + b_1^2 D_{46} = a_0 D_{54} + b_0 D_{45}, \qquad (124)$$

$$a_0^2 D_{64} = b_0^2 D_{46}, \quad a_1^4 D_{62} = b_1^4 D_{26}, \quad a_1^4 D_{51} + b_1^4 D_{15} = a_0^2 D_{31} + b_0^2 D_{13}, \qquad (125)$$

while T_{160}, T_{142}, T_{150}, T_{141}, T_{250}, T_{241}, T_{230}, T_{221}, T_{460}, T_{442}, T_{430}, T_{421} give

$$a_1 D_{70} + b_1 D_{61} = b_0^4 D_{64},\ a_1 D_{52} + b_1 D_{43} = b_0^4 D_{46},\ b_1 D_{51} = b_0^4 D_{54},\ a_1 D_{51} = b_0^4 D_{45},\ (126)$$
$$a_1^2 D_{70} + b_1^2 D_{52} = b_0 D_{51},\ a_1^2 D_{61} + b_1^2 D_{43} = a_0 D_{51},\ b_1^2 D_{32} = b_0 D_{31},\ b_1^2 D_{23} = a_0 D_{31},\ (127)$$
$$a_1^4 D_{70} + b_1^4 D_{34} = b_0^2 D_{32},\ a_1^4 D_{61} + b_1^4 D_{25} = b_0^2 D_{23},\ b_1^4 D_{64} = b_0^2 D_{62},\ b_1^4 D_{46} = a_0^2 D_{62}.\ (128)$$

The relations derived from the latter by interchanging the a's and b's, D_{ij} and D_{ji}, will be designated (126′), etc. In any D_{ij} certain factors are lacking by (113), (122). Then by (126), (126′), D_{64} and D_{46} lack also the factors

$$a_0^i b_0^j,\quad ij \text{ or } ji = 70, 62, 61, 52, 51, 43, 32, 31.$$

Applying also (125_1), we have the first two of the relations

$$D_{64} = b_0^2 D,\quad D_{46} = a_0^2 D,\quad D_{62} = b_1^4 D,\quad D_{26} = a_1^4 D, \qquad (129)$$
$$D = d_1 a_0^6 b_0^2 + d_2 a_0^4 b_0^4 + d_3 a_0^4 + d_4 a_0^2 b_0^2 + d_5 a_0^2 + d_6 a_0^2 b_0^6 + d_7 a_0 + d_8 b_0^4 + d_9 b_0^2 + d_{10} b_0 + d_{11},$$

the d_i being functions of a_1, b_1. By (128_3), $(128'_4)$,

$$D_{62} = b_1^4 D + (b_0^7 - 1)\, m,\quad D_{26} = a_1^4 D + (a_0^7 - 1)\, l.$$

By $(128'_3)$ and (128_4), $a_0 l = a_0 m = 0$, $l = m = 0$, whence the final relations (129).

By (127), (127′), D_{51} and D_{15} lack also the factors

$$a_0^i b_0^j,\quad ij \text{ or } ji = 70, 64, 62, 61, 54, 52, 43, 32.$$

Applying also (123_1), we have the first two of the relations

$$D_{51} = b_0^4 E,\quad D_{15} = a_0^4 E,\quad D_{54} = b_1 E,\quad D_{45} = a_1 E, \qquad (130)$$
$$E = e_1 a_0^5 b_0^4 + e_2 a_0 b_0 + e_3 a_0 + e_4 a_0^4 b_0^4 + e_5 a_0^4 + e_6 a_0^4 b_0^5 + e_7 a_0^2 + e_8 b_0 + e_9 b_0^4 + e_{10} b_0^2 + e_{11},$$

the literal terms being the same as in D^2. By (126_3), (126_4),

$$D_{54} = b_1 E + (b_0^7 - 1)\, \varepsilon,\quad D_{45} = a_1 E + (b_0^7 - 1)\, \varepsilon_1.$$

By $(126'_3)$, $(126'_4)$, $a_0 \varepsilon_1 = a_0 \varepsilon = 0$, $\varepsilon_1 = \varepsilon = 0$, whence $(130_{3,4})$.

Similarly, by (128), (128′), D_{32} and D_{23} lack also the factors

$$a_0^i b_0^j,\quad ij \text{ or } ji = 70, 64, 61, 54, 52, 51, 43, 31.$$

Using (124_1), (127_3), $(127'_4)$, $(127'_3)$, (127_4), we get

$$D_{32} = b_0 F,\quad D_{23} = a_0 F,\quad D_{31} = b_1^2 F,\quad D_{13} = a_1^2 F, \qquad (131)$$
$$F = f_1 a_0^3 b_0 + f_2 a_0^2 b_0^2 + f_3 a_0^2 + f_4 a_0 b_0 + f_5 a_0 + f_6 a_0 b_0^3 + f_7 a_0^4 + f_8 b_0^2 + f_9 b_0 + f_{10} b_0^4 + f_{11},$$

the literal terms being the same as in E^2 or D^4.

In terms of $r = a_0 b_1 + a_1 b_0$, conditions (123_3), (124_3), (125_3) become

$$r F = r^4 D,\quad r E = r^2 D,\quad r^4 E = r^2 F,$$

of which the last follows from the first two. The first two are satisfied if and only if d_i, e_i, f_i $(i = 3, 4, 5, 8, 9, 11)$ are constant multiples* of

$$\pi = (a_1^7 - 1)(b_1^7 - 1); \tag{132}$$

$$\left.\begin{array}{c} a_1^4 d_1 = b_1^4 d_6, \quad b_1^4 d_7 = b_1 f_7 = b_1^3 e_7, \quad a_1^4 d_{10} = a_1 f_{10} = a_1^3 e_{10}, \quad a_1 e_1 = b_1 e_6, \\ a_1 f_7 + b_1 f_1 + a_1^4 d_2 + b_1^4 d_{10} = 0, \quad a_1 f_1 + b_1 f_2 + b_1^4 d_1 = 0, \\ a_1 f_6 + b_1 f_{10} + b_1^4 d_2 + a_1^4 d_7 = 0, \quad a_1 f_2 + b_1 f_6 + a_1^4 d_6 = 0, \\ a_1^2 d_7 + b_1^2 d_1 + a_1 e_2 + b_1 e_{10} = 0, \quad a_1^2 d_1 + b_1^2 d_2 + b_1 e_1 = 0, \\ a_1^2 d_6 + b_1^2 d_{10} + b_1 e_2 + a_1 e_7 = 0, \quad a_1^2 d_2 + b_1^2 d_6 + a_1 e_6 = 0. \end{array}\right\} \tag{133}$$

In the following invariants, having the D_{ij} in (112) and (114) zero,

$$H_a R^5,\ H_b R^5,\ H_a H_b R,\ R^7,\ H_b R^3,\ H_a R^3,\ H_a H_b R^2,\ H_b R^6,\ H_a R^6,$$

the coefficients of $a_2^6 b_2^4$ are, respectively,

$$\begin{array}{l} a_0^4 b_0^6 a_1^7 + a_0 b_0^2 a_1^3 b_1^4, \quad a_0^4 b_0^6 b_1^7 + b_0^3 a_1^4 b_1^3, \quad a_0^4 b_0^6 a_1^6 b_1^6, \quad a_0 b_0^2 b_1 + b_0^3 a_1, \\ b_0^3 b_1^6, \quad a_0 b_0^2 a_1^6, \quad a_0^6 b_0^4 a_1^6 b_1^3 + a_0^4 b_0^6 a_1 b_1 + a_0^2 b_0 a_1^3 b_1^6, \\ a_0^6 b_0^4 b_1^4 + a_0^2 b_0 a_1^4 b_1^7 + a_0^4 b_0^6 a_1^2 b_1^2 + b_0^3 a_1^6 b_1^5, \\ a_0^6 b_0^4 a_1^7 b_1^4 + a_0^2 b_0 a_1^4 + a_0^4 b_0^6 a_1^2 b_1^2 + a_0 b_0^2 a_1^5 b_1^6. \end{array}$$

Subtracting the products of the first by a_1^i, the second by b_1^i, the third by $a_1^i b_1^j (i, j = 0, \ldots, 6)$, we may assume that the coefficient d_2 of $a_0^4 b_0^6$ in D_{64} is a constant. Subtracting $a_1^i R^7$, $a_1^r b_1^i H_b R^3$ $(i \leqq 6,\ r \leqq 7)$, we make the coefficient d_{10} of b_0^3 in D_{64} a constant. Subtracting $a_1^i b_1^r H_a R^3$ and $b_1^{i+1} P$, where† $P = b_1 R^7 + a_1 b_1^2 H_b R^3$ has $a_0 b_0^2 b_1^2$ as the coefficient of $a_2^6 b_2^4$, we make the coefficient d_7 of $a_0 b_0^2$ in D_{64} a constant. The coefficients of $a_2^6 b_2^4$ in

$$S = H_a H_b R^2 + a_1^2 b_1^2 H_a H_b R, \qquad H_b R^6 + a_1^2 b_1^2 H_b R^5,$$
$$H_a R^6 + a_1^2 b_1^2 H_a R^5 + a_1 b_1 S$$

are $a_0^6 b_0^4 a_1^6 b_1^3 + a_0^2 b_0 a_1^3 b_1^6$, $a_0^6 b_0^4 b_1^4 + a_0^2 b_0 a_1^4 b_1^7$, $a_0^2 b_0 a_1^4 (b_1^7 - 1)$, respectively. Subtracting the products of S by $a_1^i b_1^j$ and the second by $b_1^i (i, j \leqq 6)$, we make the coefficient d_1 of $a_0^6 b_0^4$ a function of a_1 alone. Subtracting the products of the third by $a_1^i (i \leqq 6)$, we make the coefficient of $a_0^2 b_0 b_1^7$ a constant, so that in d_6 the coefficient of b_1^7 is constant. Then by (133_1),

$$d_1 = \delta_1 (a_1^7 - 1), \qquad d_6 = \delta_6 (b_1^7 - 1) \qquad (\delta_1,\ \delta_6 \text{ constants}).$$

---

* $a_1 d = b_1 d = 0$ imply that d is a constant multiple of π.

† In the last line of (82) occurs also $a_1^7 R^7$, which we may here replace by $(a_1^7 + b_1^7 + 1) R^7$ and then, in view of (68_1), by $(a_1^7 - 1)(b_1^7 - 1) R^7$. The latter is used in the next paragraph; see (140).

The d_i, other than these and the constants d_2, d_7, d_{10}, were seen to be multiples of π, defined by (132). But, by (126_1), $b_0^4 D_{64}$ has every term a multiple of a_1 or b_1. The same is true of each d_i, since a_0 and b_0 do not enter the same manner in two terms of $b_0^4 D'_{64}$, by (129_1). Hence every $d_i = 0$. Then a simple discussion of conditions (133) shows that the e_i, f_i occurring in them are all multiples of π. Hence every e_i, f_i ($i \leqq 11$) is a constant multiple of π. But by (127_1) and ($128'_2$), $a_0^2 D_{32}$ and $b_0 D_{51}$ are multiples of a_1 or b_1. As above, each $e_i = f_i = 0$. Hence

$$D_{64} = D_{62} = D_{54} = D_{51} = D_{46} = D_{45} = D_{32} = D_{31} = D_{26} = D_{23} = D_{15} = D_{13} = 0, \qquad (134)$$

No term of ϕ *has a factor* $a_0^6 b_0^4, \ldots, a_0 b_0^3$. (135)

With the vanishing D's deleted, T_{130}, T_{121}, T_{260}, T_{242}, T_{450}, T_{441} give

$$a_0^4 D_{70} = b_0^4 D_{34}, \quad a_0^4 D_{61} = b_0^4 D_{25}, \quad a_0 D_{70} = b_0 D_{61}, \qquad (136)$$

$$a_0 D_{52} = b_0 D_{43}, \quad a_0^2 D_{70} = b_0^2 D_{52}, \quad a_0^2 D_{61} = b_0^2 D_{43}. \qquad (137)$$

The possible factors $a_0^i b_0^j$ are now those in which i, j are

$$\left.\begin{matrix} 70,\ 61,\ 60,\ 52,\ 50,\ 44, \ldots 40,\ 34,\ 30,\ 25,\ 24,\ 22,\ 21,\ 20, \\ 16,\ 14,\ 12,\ 11,\ 10,\ 07, \ldots,\ 00. \end{matrix}\right\} \qquad (138)$$

By (136_3), D_{70} cannot contain $a_0^i b_0^j$, $ij = 60, \ldots, 10, 44, 42, 24, 22, 14, 06, 04$. By ($137_2$), also 41, 21, 11, 01, 05 are absent; by (136_1), also 12, 03, 02. Hence

$$D_{70} = \sum_{i=1}^{7} g_i a_0^{7-i} b_0^i + g_0 (a_0^7 - 1) \qquad (g\text{'s functions of } a_1, b_1).$$

Then by (136_3),

$$D_{61} = \sum_{i=1}^{7} g_i a_0^{8-i} b_0^{i-1} + g_8 (b_0^7 - 1) \equiv \sum_{j=1}^{7} g_{j+1} a_0^{7-j} b_0^j + g_1 a_0^7 - g_8.$$

By (137_3), $a_0^2 (g_1 a_0^7 - g_8) = 0$, $g_8 = g_1$. Then (137_2) gives

$$D_{52} = \sum_{i=1}^{7} g_i a_0^{9-i} b_0^{i-2} + g_9 (b_0^7 - 1) \equiv \sum_{j=1}^{7} g_{j+2} a_0^{7-j} b_0^j + g_2 a_0^7 - g_9.$$

By (137_1), $a_0 (g_2 a_0^7 - g_9) = 0$, $g_9 = g_2$, and

$$D_{43} = \sum_{i=1}^{7} g_{i+2} a_0^{8-i} b_0^{i-1} + g_{10} (b_0^7 - 1) \equiv \sum_{j=1}^{7} g_{j+3} a_0^{7-j} b_0^j + g_3 a_0^7 - g_{10}.$$

By ($136'_1$), $g_{10} = g_3$. Similarly, by (136_1),

$$D_{34} = \sum_{i=1}^{7} g_i a_0^{11-i} b_0^{i-4} + g_{11} (b_0^7 - 1) \equiv \sum_{j=1}^{7} g_{j+4} a_0^{7-j} b_0^j + g_4 a_0^7 - g_{11}.$$

By ($137_1'$), $g_{11}=g_4$, and

$$D_{25}=\sum_{i=1}^{7} g_{i+4}\,a_0^{8-i}\,b_0^{i-1}+g_{12}\,(b_0^7-1)\equiv\sum_{j=1}^{7} g_{j+5}\,a_0^{7-j}\,b_0^j+g_5\,a_0^7-g_{12}\,.$$

Then ($137_2'$) and ($137_3'$) give $g_{12}=g_5$ and

$$D_{16}=\sum_{i=1}^{7} g_{i+4}\,a_0^{9-i}\,b^{i-2}+g_{13}\,(b_0^7-1)\equiv\sum_{j=1}^{7} g_{j+6}\,a_0^{7-j}\,b_0^j+g_6\,a_0^7-g_{13}\,,$$

$$D_{07}=\sum_{i=1}^{7} g_{i+5}\,a_0^{9-i}\,b_0^{i-2}+g_{14}\,(b_0^7-1)\equiv\sum_{j=1}^{7} g_{j+7}\,a_0^{7-j}\,b_0^j+g_7\,a_0^7-g_{14}\,.$$

By ($136_3'$), $g_{13}=g_6$. Thus $g_{7+k}=g_k$ ($k=1,\ldots,6$). All the conditions (136)–(137′) are now satisfied. By (126_1), ($126_1'$), .., (128_1), ($128_1'$),

$$a_1\,g_i=b_1\,g_{i+1}\,,\quad a_1^2\,g_i=b_1^2\,g_{i+2}\,,\quad a_1^4\,g_i=b_1^4\,g_{i+4}\,,\tag{139}$$

for every i making no subscript >14. Conditions (126_2), ($126_2'$), .., are satisfied. By (139),

$$a_1^7\,g_1=a_1^6\,b_1\,g_2=a_1^4\,b_1\,.\,b_1^2\,g_4=b_1^3\,.\,b_1^4\,g_1\,,\quad (a_1^7+b_1^7)\,g_1=0,$$

$$g_1=\sum_{i,j}^{1,\ldots,7} c_{ij}\,a_1^i\,b_1^j+c_{00}\,(1+a_1^7+b_1^7)\quad (c\text{'s constants}).$$

In $Z_1=V_1$ and $Z_1^2=V_2$, given by (61), the coefficients of $a_2^7\,a_0^6\,b_0$ are $1+a_1^7+b_1^7$ and $a_1^6\,b_1$. Hence by subtracting constant multiples of Z_1 and $a_1^i b_1^j Z_1^2$, we may take $g_1=0$. Then by (139) for $i=1$, $b_1\,g_2=0$, $g_2=A\,(b_1^7-1)$, where A is a function of a_1 alone. By $a_1\,g_2=b_1\,g_3$, $a_1\,A$ is a multiple of b_1 and hence zero. Thus $A=l_2\,(a_1^7-1)$. Proceeding similarly, we find that (139) gives

$$g_i=l_i\,\pi\,(i=2,\ldots,7),\quad g_0=\beta\,(a_1^7-1),\quad g_{14}=\alpha\,(b_1^7-1),$$

where π is given by (132), β a function of b_1, α a function of a_1, l_i constants. Subtracting $\beta\,I_a$, in which the coefficient of $a_2^7\,(a_0^7-1)$ is $\beta\,(a_1^7-1)$, we have $g_0=0$ in D_{70}. Subtracting $\alpha\,I_b$, in which the coefficient of $b_2^7\,(b_0^7-1)$ is $\alpha\,(b_1^7-1)$, we have $g_{14}=0$ in D_{07}. In

$$\pi\,R^7=\pi\,(a_2\,b_0+b_2\,a_0)^7\tag{140}$$

the coefficient of a_2^7 is $\pi\,b_0^7$. For $r<7$, $Z_1^r=Z_r=V_r$. Hence, by (61), the coefficient of a_2^7 in $\pi\,Z_1^r$ ($1<r<7$) is $\pi\,a_0^{7-r}\,b_0^r$. By subtracting* constant

* The multiples of Z_1, .., $\pi\,Z_6$ used in this paragraph are linearly independent combinations of the invariants (77), with $Z_1{}^m$ deleted.

multiples of these and πR^7, we have $g_i = 0$ $(i = 2, .., 7)$ in D_{70}. Hence every $g_i = 0$,

$$D_{70} = D_{61} = D_{52} = D_{43} = D_{34} = D_{25} = D_{16} = D_{07} = 0, \tag{141}$$

$$\textit{No term of } \phi \textit{ has a factor } a_0^{7-i} b_0^i \ (i = 0, .., 7). \tag{142}$$

From the latter and (138), the possible factors $a_0^i b_0^j$ now have

$$i, j = 60, .., 00, 06, .., 01, 44, 42, 41, 24, 22, 21, 14, 12, 11; \tag{143}$$

while D_{ij} vanishes unless i, j is one of these pairs. Then T_{kl0} $(k, l = 1, 2, 4)$ give

$$a_0^4 D_{50} + b_0^4 D_{14} = b_1 D_{11}, \quad a_1 D_{50} + b_1 D_{41} = b_0^4 D_{44}, \quad a_1 D_{30} + b_1 D_{21} = a_0^4 D_{60} + b_0^4 D_{24}, \tag{144}$$

$$a_0 D_{30} + b_0 D_{21} = b_1^2 D_{22}, \quad a_1^2 D_{30} + b_1^2 D_{12} = b_0 D_{11}, \quad a_1^2 D_{60} = b_1^2 D_{42} = a_0 D_{50} + b_0 D_{41}, \tag{145}$$

$$a_0^2 D_{60} + b_0^2 D_{42} = b_1^4 D_{44}, \quad a_1^4 D_{60} + b_1^4 D_{24} = b_0^2 D_{22}, \quad a_1^4 D_{50} + b_1^4 D_{14} = a_0^2 D_{30} + b_0^2 D_{12}. \tag{146}$$

We subtract from ϕ constant multiples of invariants containing only terms (143). Subtracting $a_1^r b_1^s R^3$ $(r, s \leqq 7)$, we delete b_0^6 in D_{60}. The coefficients of a_2^6 in $H_a R$ and $R^5 + a_1^4 b_1^4 R^3$ are $a_0^4 b_0^2 a_1^6$, $a_0^4 b_0^2 b_1$. Subtracting the product of the first by $a_1^i b_1^r$ and the product of the second by b_1^{i+1} $(i \leqq 6, r \leqq 7)$, we make the coefficient of $a_0^4 b_0^2$ in D_{60} a constant. The coefficients of a_2^6 in $h = H_a R^2 + a_1^2 b_1^2 H_a R$ and $\rho \equiv R^6 + a_1^2 b_1^2 R^5$ are $a_0^6 a_1^6 b_1^4 + a_0^2 b_0^4 a_1^3$ and $a_0^6 b_1^5 + a_0^2 b_0^4 a_1^4 b_1$; subtracting $a_1^i b_1^j h$ and $b_1^{i+1} \rho$ $(i, j \leqq 6)$, we make the coefficient of a_0^6 in D_{60} a function of a_1 only; subtracting $a_1^i (b_1^7 - 1) h$, we make the coefficient of $a_0^2 b_0^4 b_1^7$ a constant.

The following invariants, free of a_2^6, have the indicated coefficients of b_2^6:

$$H_b R: \ a_0^2 b_0^4 b_1^6; \quad r \equiv H_b R^2 + a_1^2 b_1^2 H_b R: \ a_0^4 b_0^2 b_1^3 + b_0^6 a_1^4 b_1^6;$$
$$a_1^6 (R^5 + a_1^4 b_1^4 R^3) + b_1 H_a R: \ a_0^2 b_0^4 a_1^7; \quad a_1 \rho + a_1^2 b_1 h: \ b_0^6 a_1^6 + a_0^4 b_0^2 a_1^2 b_1^4.$$

Subtracting the product of the first by $a_1^r b_1^i$, the third by a_1^i $(i \leqq 6, r \leqq 7)$, we make the coefficient of $a_0^2 b_0^4$ in D_{06} a constant. Subtracting the product of the second by $a_1^i b_1^j$, the fourth by a_1^i $(i, j \leqq 6)$, we make the coefficient of b_0^6 in D_{06} a function of b_1. Subtracting $b_1^j (a_1^7 - 1) r$, we make the coefficient of $a_0^4 b_0^2 a_1^7$ a constant.

The following invariants are free of a_2^6 and b_2^6:

$$H_a H_b, \quad H_a R^4 + a_1^4 b_1^4 h, \quad H_b R^4 + a_1^4 b_1^4 r,$$

and have $a_0^4 b_0^4 a_1^6 b_1^6$, $a_0^4 b_0^4 a_1^7$, $a_0^4 b_0^4 b_1^7$ as coefficients of $a_2^4 b_2^4$. Subtracting their products by $a_1^i b_1^j$, a_1^i, b_1^i $(i, j \leqq 6)$, we make the coefficient of $a_0^4 b_0^4$ in D_{44} a constant, necessarily zero by (144_2).

By (144_2) and $(144'_2)$, $b_0^4 D_{44}$ and $a_0^4 D_{44}$ involve only the $a_0^i b_0^j$ given by (143). Also $a_0^4 b_0^4$ has been deleted. Hence

$$D_{44} = h_2 a_0^4 + h_3 a_0^2 + h_4 a_0 + h_4 b_0^4 + h_6 b_0^2 + h_7 b_0 + h_8 .$$

Then, since D_{60} lacks b_0^6, (146_1) gives $b_1 h_8 = 0$ and

$$D_{60} = b_1^4 h_4 a_0^6 + d_1 a_0^4 b_0^2 + d_2 a_0^2 b_0^4 + d_3 a_0^2 b_0^2 + b_1^4 h_2 a_0^2 + d_4 a_0 b_0^2 + d_5 b_0^4 + d_6 b_0^3 + d_7 b_0^2 + b_1^4 h_3 ,$$
$$D_{42} = d_1 a_0^6 + d_2 a_0^4 b_0^2 + d_3 a_0^4 + d_4 a_0^3 + d_5 a_0^2 b_0^2 + d_6 a_0^2 b_0 + d_7 a_0^2 + b_1^4 h_5 b_0^2 + b_1^4 h_7 b_0^6 + b_1^4 h_6 .$$

Similarly, $(146'_1)$ gives $a_1 h_8 = 0$ and

$$D_{24} = a_1^4 h_4 a_0^6 + e_1 a_0^4 b_0^2 + e_2 a_0^2 b_0^4 + e_3 a_0^2 b_0^2 + a_1^4 h_2 a_0^2 + e_4 a_0 b_0^2 + e_5 b_0^6 + e_6 b_0^4 + e_7 b_0^3 + e_8 b_0^2 + a_1^4 h_3 ,$$
$$D_{06} = e_1 a_0^6 + e_2 a_0^4 b_0^2 + e_3 a_0^4 + e_4 a_0^3 + e_5 a_0^2 b_0^4 + e_6 a_0^2 b_0^2 + e_7 a_0^2 b_0 + e_8 a_0^2 + a_1^4 h_5 b_0^2 + a_1^4 h_7 b_0^6 + a_1^4 h_6 .$$

In view of the above simplification of D_{60} and D_{06} by subtracting invariants, $b_1^4 h_4 = 0$, $a_1^4 h_7 = 0$, d_1 and e_5 are constants, the coefficient of b_1^7 in d_2 and that of a_1^7 in e_2 are constants. The second members of (144_3) and $(144'_3)$ must involve only the $a_0^i b_0^j$ in (143). Hence

$$e_1 = e_3 = e_4 = e_6 = e_7 = 0, \quad d_3 = d_4 = d_5 = d_6 = 0, \quad e_2 = b_1^4 h_7 , \quad d_2 = a_1^4 h_4 .$$

Since $b_1^4 h_4 = 0$, $h_4 = A(b_1^7 - 1)$, A being a function of a_1 only. Then $d_2 = a_1^4 A(b_1^7 - 1)$. But the coefficient of b_1^7 in d_2 is a constant. Thus $a_1^4 A = 0$, so that A is a constant multiple of $a_1^7 - 1$. Hence $h_4 = c\pi$, π defined by (132). Similarly, $h_7 = k\pi$, where c and k are constants. Thus $e_2 = 0$, $d_2 = 0$. Also, $h_8 = l\pi$, l a constant. Since the terms of left member of (144_3) are multiples of a_1 or b_1, the constants d_1 and e_5 vanish; in fact, each enters a single term on the right. Hence

$$D_{60} = b_1^4 h_2 a_0^2 + d_7 b_0^2 + b_1^4 h_3 , \quad D_{42} = d_7 a_0^2 + b_1^4 h_5 b_0^2 + b_1^4 h_6 ,$$
$$D_{24} = a_1^4 h_2 a_0^2 + e_8 b_0^2 + a_1^4 h_3 , \quad D_{06} = e_8 a_0^2 + a_1^4 h_5 b_0^2 + a_1^4 h_6 .$$

Then (146_2) and $(146'_2)$ give

$$b_0^2 D_{22} = b_0^2 \sigma, \quad a_0^2 D_{22} = a_0^2 \sigma, \quad \sigma = a_1^4 d_7 + b_1^4 e_8 .$$

Hence $D_{22} = \sigma + m(a_0^7 - 1)(b_0^7 - 1)$. But $a_0^7 b_0^7$ does not occur. Hence $D_{22} = \sigma$. The terms of the left members of (145_1), $(145'_1)$ are multiples of a_0 or b_0. Hence $b_1 D_{22} = 0$, $a_1 D_{22} = 0$, $D_{22} = d\pi$, where d is a constant. Then $\sigma = d\pi$ gives $d = 0$.

In view of (143) and $D_{22} = 0$, (145_1) and $(145'_1)$ show that D_{30} and D_{12} are linear homogeneous functions of $a_0^4 b_0$; $a_0^2 b_0$, $a_0 b_0^2$, $a_0 b_0$, b_0^5, b_0^3, b_0^2, b_0; and

D_{03}, D_{21} of $a_0 b_0^4$, $a_0 b_0^2$, $a_0^2 b_0$, $a_0 b_0$, a_0^5, a_0^3, a_0^2, a_0. But the right members of (146_3) and $(146_3')$ must involve only (143). Hence

$$D_{30} = \alpha a_0^2 b_0 + \beta b_0^3 + \gamma b_0, \quad D_{21} = \alpha a_0^3 + \beta a_0 b_0^2 + \gamma a_0,$$
$$D_{12} = \beta a_0^2 b_0 + \mu b_0^3 + \nu b_0, \quad D_{03} = \beta a_0^3 + \mu a_0 b_0^2 + \nu a_0.$$

The left members of (144_3) and $(144_3')$ are now of degree $\leqq 3$ in a_0, b_0; their right members of degree $\geqq 4$. Hence each member is zero. Thus

$$d_7 = e_8 = 0, \quad \alpha, \beta, \gamma, \mu, \nu, \quad h_2, h_3, h_5, h_6$$

are constant multiples of π.

In particular, D_{60}, D_{42}, D_{24}, D_{06} now vanish. By (144_2), every term of $b_0^4 D_{44}$ must be a multiple of a_1 or b_1; but each h_i is a constant multiple of π. Hence $D_{44} = 0$. Similarly, by (146_3), α, γ, μ, ν vanish. After subtracting βR^5, we have $\beta = 0$, since

$$\pi R^5 = \pi (a_2^2 b_0^2 + b_2^2 a_0^2)(a_2 b_0 + b_2 a_0).$$

Thus D_{30}, D_{21}, D_{12}, D_{03} now vanish. Then $D_{11} = 0$ by (145_2), $(145_2')$. In view of the eleven D's just proved zero and (143), the possible factors $a_0^i b_0^j$ are now

$$i, j = 50, 41, 40, 20, 14, 10, 05, 04, 02, 01, 00. \qquad (147)$$

Hence by (144_1) and $(144_1')$, D_{50} and D_{41} involve only 41, 14, 05, 04; D_{14} and D_{05} only 50, 41, 40, 14. Applying also (145_3) and $(145_3')$, we get

$$D_{50} = sb_0^5, \quad D_{41} = sa_0 b_0^4, \quad D_{14} = sa_0^4 b_0, \quad D_{05} = sa_0^5.$$

By (144_2), s is a multiple of π. But

$$\pi R^6 = \pi (a_2 b_0 + b_2 a_0)(a_2^4 b_0^4 + b_2^4 a_0^4).$$

Hence by subtracting sR^6, we make $s = 0$. Thus by (147),

$$i, j = 40, 20, 10, 04, 02, 01, 00 \qquad (148)$$

give the only non-vanishing D_{ij} and the possible factors $a_0^i b_0^j$. Then T_{k00}, $k = 1, 2, 4$, give

$$\begin{gathered} a_1 D_{10} + b_1 D_{01} = a_0^4 D_{40} + b_0^4 D_{04}, \quad a_1^2 D_{20} + b_1^2 D_{02} = a_0 D_{10} + b_0 D_{01}, \\ a_1^4 D_{40} + b_1^4 D_{04} = a_0^2 D_{20} + b_0^2 D_{02}. \end{gathered} \qquad (149)$$

The second members must involve only the $a_0^i b_0^j$ given by (148). Hence

$$D_{40} = pa_0^4 + qb_0^4 + r, \quad D_{10} = Pa_0 + Qb_0 + U, \quad D_{20} = \rho a_0^2 + \sigma b_0^2 + \lambda,$$
$$D_{04} = qa_0^4 + sb_0^4 + t, \quad D_{01} = Qa_0 + Sb_0 + T, \quad D_{02} = \sigma a_0^2 + \mu b_0^2 + \nu.$$

Then relations (149) are satisfied if, and only if,

$$r = t = U = T = \lambda = \nu = 0, \quad p = a_1 P + b_1 Q, \quad s = a_1 Q + b_1 S, \tag{150}$$

$$P = a_1^2 \rho + b_1^2 \sigma, \quad S = a_1^2 \sigma + b_1^2 \mu, \quad \rho = a_1^4 p + b_1^4 q, \quad \mu = a_1^4 q + b_1^4 s. \tag{151}$$

Subtracting $a_1^i b_1^r H_a$, $b_1^{i+1} R^4$ ($i \leqq 6$, $r \leqq 7$, we have $p =$ constant. Subtracting $a_1^r b_1^s R^2$, we have $q = 0$. In $a_1(R^4 + a_1^4 b_1^4 R^2) + a_1^2 b_1 H_a$ and H_b, the coefficients of a_2^4 are zero; those of b_2^4 are $b_0^4 a_1^2$ and $b_0^4 b_1^6$. Subtracting the product of the first by a_1^i, the second by $a_1^r b_1^i$, we make $s =$ constant. Subtracting $a_1^r b_1^s R$, which is free of a_2^4, b_2^4, we make $\sigma = 0$. Then (151) becomes

$$\rho = p a_1^4, \quad \mu = s b_1^4, \quad P = p a_1^6, \quad S = s b_1^6.$$

The final conditions (150) give

$$b_1 Q = p(a_1^7 + 1), \quad a_1 Q = s(b_1^7 + 1).$$

Since p and s are constants, we have $p = s = 0$, $Q = c\pi$. Hence

$$\phi = c\pi(a_2 b_0 + b_2 a_0) + D_{00}.$$

We make $c = 0$ by subtracting $c\pi R^4$, since

$$\pi R^4 = \pi(a_2 b_0 + b_2 a_0).$$

Hence ϕ is now D_{00} and therefore by (56), a function of a_1, b_1 only.

In view of the last two foot-notes, it is readily seen that the invariants, which have been subtracted from ϕ to reduce it to $\Sigma a_1^r b_1^s$, together with the latter, are linearly equivalent to the set (82).

THEOREM. *Every invariant of a pair of quadratic forms in the* $GF[2^3]$ *is an integral function of the eight independent invariants* (81); *indeed a linear combination of the linearly independent invariants* (82), *for* $n = 3$.

THE UNIVERSITY OF CHICAGO, *October*, 1908.